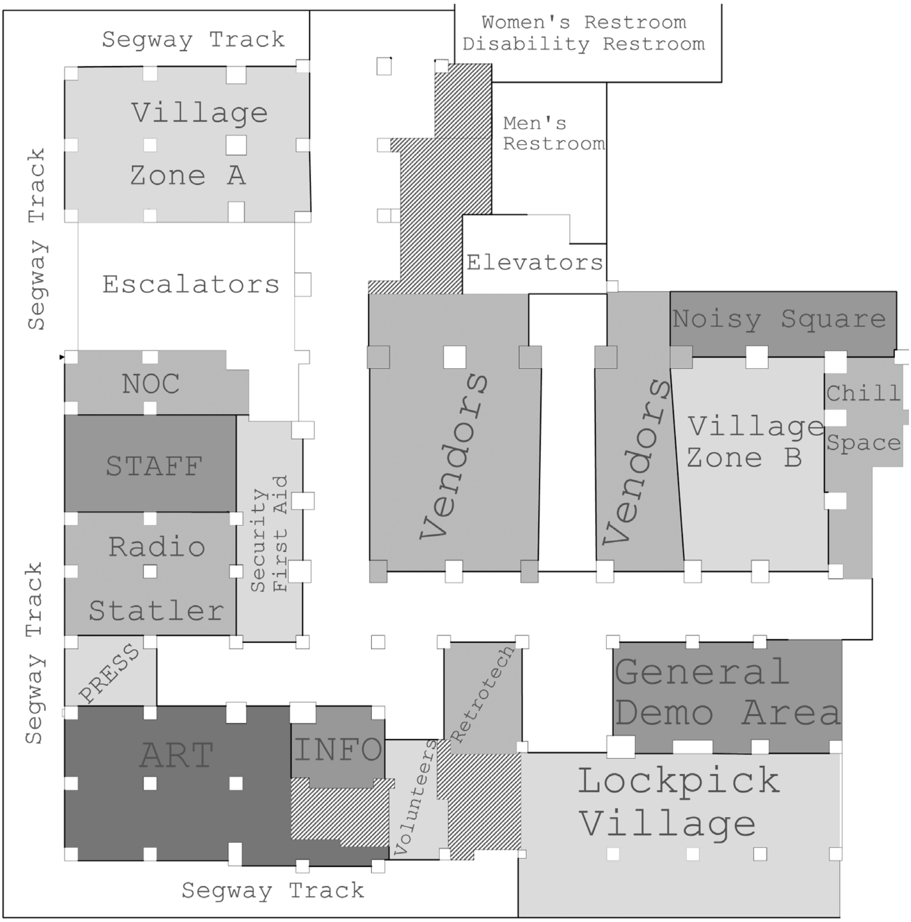
HOPE X

PROGRAM

SECOND FLOOR



Flip to the inside back cover for eighteenth floor information

HOPE X

Welcome to HOPE X! It's our tenth conference, and the 20th anniversary of Hackers On Planet Earth. We've come such a long way and it all just keeps getting more exciting.

It's also the 30th anniversary of *2600 Magazine*, which makes all of this possible, along with literally hundreds of volunteers, coordinators, speakers, artists, vendors, and overall cool people. You may have heard that *2600*'s biggest distributor went bust and apparently won't be paying a huge sum that they owe. This could have put a real damper on this event, but such challenges are nothing the hacker community isn't familiar with. We've seen a tremendous outpouring of support and that ensures that not only will the conference go on as planned, but it will be bigger and better than ever.

Our theme this year is dissent and do we have plenty of that! There are more talks on ways to fight surveillance than have probably ever occurred under one roof before. We have some of the most qualified people on the planet here to share their expertise and hopefully help us all make significant changes in the way society works. Special thanks go out to Daniel Ellsberg and Edward Snowden for the inspiration - and for doing the right thing when it mattered the most. The hacker community is filled with idealistic and intelligent people of all ages and HOPE X is where we can all learn that we're not alone.

We are issuing special police badges to all of our attendees and we ask that you wear them at all times when attending talks and events within HOPE. We're expecting bigger crowds than ever this year, so please don't fret if you're not able to make it to all of the talks you want to see. The bigger ones will be simulcast and there will always be something else to see. Not to mention that it'll all be available digitally. We guarantee you'll have a great time as long as you expect and embrace the unexpected and unplanned. That's how we all got here.

There are many conferences going on but HOPE is one of those unique ones where people from all different communities mix and share ideas and experiences. This makes us very happy and proud. It shows how the hacker community has grown and how relevant the hacker perspective truly is. So check out talks that teach you something new or that come from a totally different angle than what you're used to. We know you'll be amazed. And, of course, try to meet as many people as you can throughout the event. Lifetime friends are made here. Even a few marriages.

While talks are the major attraction, there is so much else going on at HOPE, on four separate floors of the hotel. We're having concerts on the first floor, workshops and seminars on the sixth floor, amateur radio and *2600* merchandise on the 18th floor, and of course, everything that's happening on the second floor. Yes, the second floor is the hub of hacker activity for the weekend. You'll find everything from a lockpick village to hardware hacking to a huge hackersoace area to chill zones and Segway rides. This is also where you'll find the biggest stash of Club-Mate in the country, along with all kinds of other really cool stuff of interest to hackers in our vendor area.

We want to thank our many volunteers for making all of this possible. Remember, it's impossible to do what we do - we've been told this many times. Yet, we do it time after time because of the magic of this community. It's not too late for you to get involved - just stop by the InfoDesk on the second floor and say you want to help. You'll have a blast.

As you can see, the hotel has been saved (no small thanks to HOPE attendees and our campaign to keep it standing) so the future is once again promising. Please treat the place with respect, as they are very good to us and this is our home for the weekend.

If you're not used to New York City, it's a really neat place to check out and it's all around us. Ask at the InfoDesk for nearby attractions, decent places for food, etc. And do try and stick around after the conference so you can have even more fun in the Big Apple.

One page isn't sufficient to do the entire conference justice. Which is why we hope you share your feelings afterward by emailing feedback@hope.net and let us know how your HOPE experience was. Enjoy!

TALKS

Apophenia: Hunting for the Ghost in the Machine
Wil Lindsay

This discussion will look at the practice of exposing anomalies in network communications and computer processes in order to find evidence of interference (or intentional communication) from beyond the grave. Known as Instrumental Trans-Communication (ITC), the practice has roots as far back as the 1930s and has survived into the digital era. We will look at how these same methods are now being applied to Wi-Fi networks, custom software development, remotely networked sensors, and digital spectrogram systems designed to capture images of the spirits of the deceased.

(The discussion will be accompanied by a basic circuit workshop where participants can build a simple device with accompanied software to collect data and test the methods discussed in the presentation.)

Friday 1400 Serpico

Are You Ready to SIP the Kool-Aid?
Richard Cheshire, Gaston Draque

Session Initiation Protocol (SIP) is the gateway drug to VoIP (Voice over Internet Protocol). You will see how such a phone call is set up, and will witness an in-depth discussion of Asterisk, the open source PBX software that represents the new age of telephone switching in the 21st century.

Friday 1000 Serpico

Art under Mass Surveillance
!Mediengruppe Bitnik

!Mediengruppe Bitnik are contemporary artists. In their talk, they will show two examples of their work, illustrating the translation of hacking from the computer field into an artistic practice. Bitnik will show how to hack the opera in ten easy steps and what happens when you send a parcel with a hidden live webcam to Julian Assange at the Ecuadorian Embassy in London.

Friday 2000 Serpico

Ask the EFF - This Year on the Internet
Nate Cardozo, Kurt Opsahl, Adi Kamdar, Peter Eckersley, Eva Galperin

Hear from lawyers, activists, technologists, and international policy analysts from the Electronic Frontier Foundation, the nation’s premiere digital civil liberties group fighting for freedom and privacy in the computer age. Since HOPE Number Nine, much has happened on the Internet. From Aaron Swartz’ tragic death to Edward Snowden’s revelations, from TPP to Stop Watching Us, they will put it all in context and answer your questions. This session will include updates on current EFF issues such as their efforts to end mass spying both at home and abroad, their fight against the use of intellectual property claims to shut down free speech and halt innovation, a discussion of their technology projects to protect privacy and speech online, updates on their cases against the NSA, litigation and legislation affecting security research, what EFF is doing to open access to scholarly works, how they’re fighting the expansion of the surveillance state, and much more. Half the session will be given over to Q&A, so it’s your chance to ask EFF questions about the law and technology issues that are important to you.

Saturday 1100 Manning

Barrett Brown and Anonymous:
Persecution of Information Activists
Kevin Gallagher, Ahmed Ghappour, Gabriella Coleman

Barrett Brown, a Dallas-based writer and freelance journalist, was arrested in late 2012 and indicted several times on charges including the publication of a hyperlink. He was earlier pegged by the media as an “unofficial spokesperson” for the hacktivist collective known as Anonymous. But who is he really and what was he trying to uncover that made him a target of the feds? The prosecution was widely regarded as excessive and included a gag order, subpoenas, charges issued against family members, attempts to seize defense funds, and criminal counts so flawed that they were later dismissed. This talk will explore Brown’s work, what happened during his case, the dynamics of his interactions with Anonymous and its implications for other journalists who work with hackers, and why his case outraged many of those who care for free speech and freedom of press.

Friday 1200 Manning

A Beautiful Mosaic: How to Use FOIA to Fight Secrecy, Explore History, and Strengthen American Democracy
Michael Morisy, Michael Ravnitzky

The Freedom of Information Act (FOIA) is a simple but powerful tool that permits any citizen to find out more about what their government does, permitting more informed participation in American society and government processes. This presentation will show how public records released under FOIA have been used to expose questionable surveillance programs, domestic drone programs, and even an exploding toilet. It also highlights the availability of an array of free, public resources to explore millions of pages of government records that have already been released, so you can see the results of your tax dollars at work. This talk will also review ways of overcoming some common agency roadblocks to get the records and data you want. Examples will be drawn from the GovernmentAttic.org and Muckrock.com web sites.

Two comprehensive workshops will follow: Basic FOIA Workshop, and FOIA Advanced Strategies and Tactics.

Friday 1200 Serpico

Biohacking and DIYbiology
North of the 45th Parallel
Kevin Chen, Connor Dickie, Alessandro Delfanti

In the past few years, there have been foundational developments enabling hobbyists and seasoned professionals to research and develop the life sciences outside of classical institutions. Known as DIYbiology or biohacking, this shift in the bio-world takes its inspiration from mature hacker and open source cultures. In this panel, Canadian biohacker successes and struggles will be presented. Current legal, economic, and political landscapes that affect Canadian and global biohackers will be discussed and compared. What constraints and challenges are faced when it comes to doing synthetic or molecular biology outside of its conventional confines? How is the community membership growing and what does it take to accelerate this growth? Lastly, what growth are we anticipating for independent and open biotech research, as well as inter-laboratory and international collaboration? And how can the audience and other hacker communities get involved in this exciting shift?

Saturday 2000 Manning

Bless the Cops and Keep Them Far from Us: Researching, Exploring, and Publishing Findings While Staying out of Legal Trouble

Alexander Muentz

We all like to tinker and explore. Hacking, exploring, and publishing findings is important to our community as well as the world at large. Unfortunately, law enforcement and the operators of the systems you investigate may disagree and use the legal system to threaten or silence you. How can hackers, pen testers, and security researchers all protect themselves? Can you reverse engineer a device you just purchased? Can you investigate a security hole in another's web server? What can you tell others about your findings? This talk will consider how current U.S. laws affect one's ability to explore systems, collaborate, and publish findings. Q&A will follow.

Saturday 1000 Manning

Blinding The Surveillance State

Christopher Soghoian

We live in a surveillance state. Law enforcement and intelligence agencies have access to a huge amount of data about us, enabling them to learn intimate, private details about our lives. In part, the ease with which they can obtain such information reflects the fact that our laws have failed to keep up with advances in technology. However, privacy enhancing technologies can offer real protections even when the law does not. That intelligence agencies like the NSA are able to collect records about every telephone call made in the United States or engage in the bulk surveillance of Internet communications is only possible because so much of our data is transmitted in the clear. The privacy enhancing technologies required to make bulk surveillance impossible and targeted surveillance more difficult already exist. We just need to start using them.

Sunday 1700 Manning

Bootkits: Step-by-Step

Eric Koeppen

Basic Input/Output System (BIOS) is firmware that boots older machines. Unified Extensible Firmware Interface (UEFI) is a combination of firmware and a boot-loader that boots newer machines. As a result of the leaks by Edward Snowden, the possible existence of rootkits that can affect the BIOS and UEFI has been widely reported. Both of these technologies exist in memory that is not typically accessible remotely, which makes infection particularly difficult. The location of these technologies is even difficult to reach by the operating system, which makes detection of such an infection at this level also a difficult problem. This talk will explore all of the steps that need to take place in order to accomplish this feat, review creative measures malware has taken to tackle these problems, and review methods for detection of these kinds of infections.

Sunday 1200 Olson

Bringing Down the Biological System: How Poisons Hack the Body

Jennifer Ortiz

Poisons can kill... but how? Why are some chemicals beneficial in small quantities but lethal in large amounts? How does a sometimes miniscule amount of chemical bring the whole system down? And how can these processes be counteracted such that the system may survive? Learn about how the complex cellular network of our body works and what happens when this network is disrupted.

Sunday 1100 Serpico

Building an Open Source Cellular Network at Burning Man

Johnny Diggz, Willow Brugh

There is literally nowhere else on earth where you can run an experimental mobile phone network with a potential 50,000 users and get away with it (legally). Nowhere else can you learn so much in as short a timeframe about people's relationships with their mobile phones or what makes a mobile network tick. Since 2006, the folks behind OpenBTS have been running the Papa Legba camp at Burning Man, providing fully licensed independent (free) GSM cellular service in the most unlikely of places. Johnny and Willow will go through the hardware and software tools they deployed in 2013, along with a discussion of lessons learned and future plans.

Friday 1900 Manning

Can You Patent Software?

Ed Ryan

Patent law is a subject of general loathing among hackers and those in the open source movement. While a few grudgingly agree that some things might be worthy of patents, the idea of patenting software seems to offend core values of our community. Despite that fury, it is difficult to pin down exactly what a software patent is. To what degree is a patent directed to software instead of a new and useful machine? How can you separate out those two concepts? This talk aims to present the core problems of software patents in a way that is accessible to hackers and other technologists and, in particular, will address the Alice Corp. decision by the Supreme Court in June. This talk is an academic discussion of patent law and should not be construed as legal advice.

Friday 1600 Serpico

Closing Ceremonies

Every year, people make the same mistake. They book their return trips too early on Sunday. If you've done that this year, we encourage you to pay whatever the fee is to change your ticket and stick around. The HOPE closing ceremonies are always a blast, as well as an opportunity to win lots of cool prizes that we have accumulated over time. We'll also wax sentimental about how we (hopefully) managed to pull off yet another one of these events. So stick around Sunday evening. Think of Monday as a holiday - and beg forgiveness on Tuesday.

Sunday 1900 Manning

Codesigning Countersurveillance

Sasha Costanza-Chock

Recent revelations about massive data collection by the National Security Administration have brought sustained popular attention to the rise of pervasive

surveillance systems. We have entered a moment of important dialogue about the surveillance state, the role and ethics of technology companies, the potential harms of mass surveillance to civil liberties and human rights, and the need for interventions involving technology, policy, and social practice. At the same time, the voices of communities that have long been most explicitly targeted by surveillance have been largely excluded from the debate. There are multiple, overlapping surveillance regimes, and they disproportionately target people of color, low-income, and working people, as well as activists in general. State, military, and corporate surveillance regimes are growing in scope, power, and impunity, not only in countries such as Iran, Syria, and China, but also within liberal democracies such as the United States, India, and Brazil. This talk will focus on projects and process from the MIT Civic Media Codesign Studio (codesign.mit.edu), which works with community-based organizations to develop civic media projects that connect to grounded strategies for social transformation.
Saturday 2200 Olson

Community Infrastructure for FOSS Projects

James Vasile

At HOPE Number Nine in 2012, James spoke to people about how to build community infrastructure to provide support at a scale larger than just one project at a time. Then he went and built some. This talk is about lessons learned - how to replicate the successes and avoid the failures he's experienced in the last two years. The focus will be on his two case studies: 1) the formation of a localization community for anti-censorship and anti-surveillance tech (which went reasonably well) and 2) creating a heavier-weight code auditing organization for anti-censorship and anti-surveillance tech (which had some hiccups). There are lessons in both and they will be the basis of discussion here. The goal is to also seed some ideas on how to build this kind of infrastructure for other niches and the wider free software community.
Sunday 1600 Serpico

Community Owned and Operated Cellular Networks in Rural Mexico

Peter Bloom, Maka Muñoz

Why try to avoid them spying on us on their networks when we could just build our own? This is what the Rhizomatica project has done in rural Mexico, where they help to build and maintain community owned and operated GSM/cellular infrastructure. Come and hear about experiences in the field and how to deal with the technological, legal, social, and organizational aspects that come along with operating critical communications infrastructure from a community emancipation and autonomy perspective. If you enjoy freedom, community, and dismantling the corporations and governments that seek to monitor, control, and exploit us, then this presentation is for you. The talk will not be overly tech-focused, so don't worry if you haven't got the faintest idea or couldn't care less how a cell phone network operates. If you want tech and geekiness, you can also attend the workshop: "How to Build and Run Your Own Cellular Network."
Friday 1800 Manning

A Conversation with Edward Snowden

We had to keep this bombshell quiet til the last minute since some of the most powerful people in the world would prefer that it never take place. (Even at this stage, we wouldn't be surprised at mysterious service outages, but we believe the hacker spirit will trump the unprecedented might of the world's surveillance powers. Fingers crossed.)

Daniel Ellsberg has been an inspiration to Edward Snowden and Ellsberg himself has expressed his admiration of Snowden's actions in releasing information revealing the extent of NSA's spying on civilians around the globe, including within the United States. Ellsberg changed the conversation in the height of the Vietnam War through the Pentagon Papers - by revealing deceptive practices by the government. Snowden has also dramatically changed the conversation on surveillance and intelligence-gathering with his revelations.

We're honored and proud to have HOPE be the forum via which these two American heroes converse. Snowden is, of course, still unable to leave Russia because of the threat he faces from the authorities in the United States. So he will be joining us and speaking on a video link right after Daniel Ellsberg's keynote.
Saturday 1400 Manning, Serpico, Olson

Crypto for Makers: Projects for the BeagleBone, Pi, and AVRs

Josh Datko

As more devices join the Internet of Things, it is increasingly important that these devices remain protected from surveillance and compromise. This talk will show how to add specialized, commercially available, crypto Integrated Circuits (ICs) to improve the security of your BeagleBone, Pi, or AVR based platform. ICs such as a Trusted Platform Module, I2C authentication chips, and hardware random number generators will be discussed. The CryptoCape, an Open Source Hardware daughterboard, made in collaboration between SparkFun Electronics and the presenter, will be presented in detail. Lastly, this talk will describe the experience of running a Tor relay on a BeagleBone Black for over 200 days.
Friday 2100 Olson

Cultures of Open Source: A Cross-Cultural Analysis

Sandra Ordonez, Bryan Nunez, Douwe Schmidt

While a common philosophical and cultural thread ties all of us in open source together, the ecosystem is as diverse as the world itself. In fact, open source projects are a kaleidoscope of cultures that influence how they are approached, how teams interact, outcomes, and what type of people they attract. At the same time, open source is suffering greatly from a lack of diversity. Three percent are women, and many users from non-English subgroups feel their voices are not heard in the OS ecosystem. This panel will discuss: how open source projects can build bridges to help incorporate people from non native English speaking communities, examples of when lack of cross-cultural sensitivity goes wrong, descriptions of patterns and regional differences observed in various open source communities, and why the Dutch are some of the best open source volunteers ever.
Sunday 1500 Manning

Cyber Security in Humanitarian Projects as a Social Justice Issue

Lisha Sterling

Without secure code and implementation, humanitarian projects can be used against the very people

they are designed to help. This is a basic problem of social justice. If security is only available to people with money, privilege, and the fortune to not be in the midst of a disaster, then there is no security. As Internet crime rises and security solutions gain momentum, vulnerable populations are left out of the protection that the privileged few enjoy. Issues of trust, budgetary restrictions limiting low-barrier digital security tools, and the mass surveillance/digital disenfranchisement of the non-elite are the obstacles to a secure commons. Community building and resource sharing on the Internet is only accomplished when we take part in building social justice by using our skills to improve open source code security and its implementation across the humanitarian ecosystem.
Sunday 1000 Serpico

Dark Mail

Ladar Levison, Stephen Watt

The Dark Mail Initiative represents a collaborative effort to bring about a new generation of standards designed to provide automatic end-to-end encryption for email. The presentation will cover the "dmail" architecture, with a focus on the key elements of the design that allow it to overcome some of the most problematic traditional usability issues, all the while preserving a world-class guarantee of security. Dark Mail stands in a unique position against most competing technologies because of its commitment to complete transparency, both in the proposed open dmail specifications and in the open source implementation that is targeted for release later this year. The talk will also include a short discussion of the Lavabit legal saga that precipitated the dmail development effort, the design goals of the project, and an explanation of why these goals are important, both to the computer security community and to society at large. The discussion will conclude with a short update on the status of the reference implementation development effort.
Friday 2100 Manning

Disruptive Wearable Technology

Becky Stern

As technology becomes ever more embedded in the fabric of our society and even our clothes, we must grapple with ever more complicated tradeoffs regarding privacy and security. This talk will highlight disruptive wearable technologies that creatively and assertively address these modern technological and societal changes. Come learn about underwear that that tattles on a TSA agent's wandering fingers during a secondary screening, makeup that makes you imperceptible to facial recognition software, and eye-tracking glasses that let a paralyzed graffiti writer tag again. Most projects featured are open source or how-to guides, and span the last ten years. Becky Stern's intention is to inspire HOPE X attendees to think more about the physical body as a canvas for hacking, social engineering, fashion, and wearable tech.
Saturday 1500 Manning

DIY Usability Research: A Crash Course in Guerrilla Data Gathering

Kaytee Nesmith

Good news: it's becoming abundantly clear that more and more people want to use surveillance circumvention tools to protect their privacy. Bad news: most people can't figure out how to use them. Thankfully, usability research is no longer difficult to arrange or afford. Anyone - developers, designers, and project managers alike - can conduct user testing at any time, in any setting. In this presentation, you will learn everything you need to know to get started on your own qualitative user research, how it can help you understand and solve for your users' needs, and what it means for the future of surveillance circumvention technology.
Saturday 1900 Olson

Drop It Like It's Hot: Secure Sharing and Radical OpSec for Investigative Journalists

Harlo Holmes, Aurelia Moser, Bart Gellman

As developer-journalists, Harlo and Aurelia work with sensitive information about critical investigations of governments, institutions, and individuals - domestic and foreign. Bart Gellman of the *Washington Post* is one of three journalists who received classified NSA archives from Edward Snowden. The security and reliability of the information these panelists handle is of the utmost importance. Managing their resources and notes while maintaining the privacy and safety of their sources can be complicated as they work on collaborative teams of varying technical and subject expertise. This talk will go over how journalists collaborate covertly in the newsroom, reviewing some tools and applications for dead-dropping data, and protecting privacy where possible, at places like the *Washington Post*, the Guardian Project, the *New York Times*, Ushahidi, and Internews Kenya.
Sunday 1500 Serpico

Echoes of Returns Lost: The History of *The Telecom Digest*

Bill Horne

This talk is a brief history of the people and events which shaped The *Telecom Digest's* history, presented by its current editor. (*The Telecom Digest* is the oldest continuously running electronic magazine about telecommunications on the Internet - and one of the oldest mailing lists still on the Internet in *any* category.) Bill will discuss the previous moderators and the events that led to his stewardship. There will be anecdotes from the archives, some discussion of the personalities that formed the digest, and brief speculation about its future. There have been some truly memorable posts over the years which will be focused upon. The day-to-day workflow will be described, along with the ways things have changed over the years, from manual efforts to Usenet access to the current Majordomo II list management software. Hear about the evolution of the digest from a mostly "Bell" centered e-zine, to the Wild West days of MCI and Sprint, up to the re-consolidations now underway. In addition, Bill will explain his philosophy of moderation and the ways he goes about it while seeking to lighten the moderator's technical workload, automate manual procedures, and his preparations to adapt for the new YaGooMail "walled garden" paradigm.
Sunday 1700 Olson

Electric Waste Orchestra: Learning and Teaching Music, Electronics, Programming, and Repurposing

Colten Jackson

The technology to turn e-waste into musical instruments is free, open source, and waiting to be fully explored. At this talk, you'll learn how the computer junk piling up in IT departments everywhere can be

transformed into novel input devices, allowing kids and adults alike to create physical instruments to control electronic music.
Saturday 1700 Serpico

Elevator Hacking: From the Pit to the Penthouse
Deviant Ollam, Howard Payne

Throughout the history of hacker culture, elevators have played a key role. From the mystique of students at MIT taking late-night rides upon car tops (don't do that, please!) to the work of modern pen testers who use elevators to bypass building security systems (it's easier than you think!), these devices are often misunderstood and their full range of features and abilities go unexplored. This talk will be an in-depth explanation of how elevators work... allowing for greater understanding, system optimizing, and the subversion of security in many facilities. Those who attend will learn why an elevator is virtually no different than a staircase as far as building security is concerned!
Sunday 1200 Manning (2 hours)

Ergonomic Human Interface Hacking
Carl Haken

Do you experience numbness or weakness in your hands? Do you have a permanent case of Emacs pinky? Are you playing vi golf for your health? Since the release of the Macintosh 30 years ago, mainstream human-computer interfaces have changed little, and hardcore computer users (hackers, coders, gamers, etc.) are paying the price.

This talk will examine potential solutions to the repetitive strain injuries commonly experienced by computer users, including: head-based cursor control, ultra-ergo keyboards, foot pedals, and other optimizations.
Friday 2000 Olson

Ethical Questions and Best Practices for Service Providers in the Post-Snowden Era
Nicholas Merrill, Ladar Levison, Declan McCullagh

Service providers have always had to shoulder a tremendous ethical burden because of the volume of personal information they hold, including files, metadata, and geolocation data. Some, like Calyx and Lavabit, have been willing to take extra steps to protect their customers' privacy rights. After Edward Snowden's revelations about the U.S. government, some larger providers have become more willing to fight for their users in court or speak publicly about surveillance demands. But many court dockets remain sealed. This talk will explore the telecommunications privacy landscape as we now know it, including the extent of the surveillance regime that some of us suspected all along. The focus will be on best practices for service providers at many levels: software design, API design, network design, policy, and more.
Sunday 1100 Manning

Fuckhackerfucks! An Audience Bashing
Johannes Grenzfurthner

Johannes of art tech group monochrom will indulge in a public rant about hacker culture and why it has to be saved from itself. Expect strong language, indecency, and valid critique of the status quo of hackdom. (No wonder his 2008 Google Tech talk got censored and never made it onto Google's YouTube channel.)
Sunday 1300 Serpico

G-code: The Programming Language of Machining and 3D Printers
Todd Fernandez

This talk will provide an explanation of the G programming language commonly known as "G-code." G-code was originally developed in the 1950s to allow numerical control of industrial manufacturing equipment. G-code's major user base is not traditional programmers or software engineers, but machinists, manufacturing programmers, and those who own 3D printers. In modern times, it is used to control everything from a home-built RepRap to massive CNC milling machines to make anything you could possibly imagine.
Friday 1800 Olson

(Geo)location, Location, Location: Technology and Countermeasures for Mobile Location Surveillance
Matt Blaze

We all know that law enforcement (and private companies, for that matter) can track you through your mobile phone. But how exactly does tracking work? How precise are they? When can they get this data? And is there anything you can do to obscure your movements without moving into a Faraday cage? This talk will discuss the various technologies that law enforcement, intelligence agencies, and private industry use to track individual movements. There are a surprising number of different techniques. Many involve the signals emanating from - and records created by - mobile phones, but there are more specialized - and surprising - tracking techniques in use as well. The tower data information contained in cellular call detail records, E911 "pings," tower dumps, IMSI catchers, aggregate metadata analysis, Wi-Fi and Bluetooth-based locators, traditional RF and GPS trackers, and some of the sophisticated "implants" used by intelligence agencies will all be discussed. Can you opt out without opting out of the Information Age? Not always, but there are a few countermeasures that work, as well as a surprising number that don't. There will be an analysis of a number of real-world cases of tracking, as well as tips on how to learn from the mistakes of others.
Saturday 1500 Serpico

The Hacker Wars - A Conversation with NSA Whistleblower Thomas Drake
Thomas Drake, Vivien Lesnik Weisman

Vivien Lesnik Weisman, director of the upcoming documentary film *The Hacker Wars*, speaks with Drake on the confluence of hacktivism and whistleblowing. Depending on one's perspective on who should regulate information, hacktivists and whistleblowers are either criminals or freedom fighters. Drake will discuss his own case and the dystopian dynamic that ensued when the criminal justice system was used as an instrument to destroy him. In light of his personal experience with the state, he will discuss the importance of specific stories of young hacktivists, along with that of whistleblower Edward Snowden, including their battles with the U.S. government.
Friday 1400 Manning

Hacking Money, from Alexander the Great to Zerocoin
Finn Brunton

Cryptocurrencies are here. Bitcoin is in the news and in the courts, and many other currencies are following, offering everything from anonymous

transactions to redistributive economies to monetary sovereignty to, of course, doges. Related platforms promise to reinvent DNS, cloud storage, voting, contracts, even the corporation itself. To really understand what's happening, and how we can steer cryptocurrencies towards accomplishing social and political goals, we need to connect the breaking news with the deeper history of the technology of money. This will be a look back - before Hashcash and DigiCash, before Chaum, May, Diffie, Hellman and Merkle - and forward, into the future to plausible scenarios and speculations for launching projects now. What connects Belfast pubs in 1970 with the vault of the New York Federal Reserve, trading networks of the Islamic golden age, an Austrian ski village during a global depression, willows by the Thames, and an extraterritorial fortress on the outskirts of Singapore Changi Airport? Why are survivalists filling ammo boxes with rolls of U.S. nickels? Why do the differences in hash algorithms matter, and what covert software agreements underwrite the verification of physical bank notes? Money is one of the most significant social technologies that humans have invented, and cryptocurrencies are an opportunity to hack on the architecture of trust, verification, value, and credit that shapes how we can live. This talk, and conversation during and after, will explore what we can do with this opportunity.
Saturday 1800 Serpico

Hacking the Patent System: The Vulnerabilities That Allow for Bad Patents and How to Stop Them

Charles Duan

We are hearing about the problems of software patents everywhere: in the tech blogs, in the mainstream news, from the President, and even out of the Supreme Court. We hear stories of patent trolls destroying technology companies and small businesses with patents on such simple ideas as scanning to email or in-app purchases. How did we end up with a patent system that generates patents that become the tools of legal abuse? This talk will look at the patent system like an insecure OS, one rife with vulnerabilities in dire need of patching. Just as an unsecured computer can be misused to the ends of malicious users, vulnerabilities in the patent system allow clever lawyers and patenters to obtain patents on simple ideas, ones that anyone with an ounce of programming skill would find obvious. We will look at how to get a patent on comparing and adding two numbers - a patent that actually exists right now. We will consider the flaws in the system that allow aggressive patent holders to exploit weak patents and extract money from real innovators. And we will talk about how to fix that system - but only with the help of all of us who care about the future of technology.
Friday 1500 Serpico

Hearses and Hand-Held Calculators: The Unlikely Connections That Shaped Modern Technology and Tech Culture

Bill Degnan

Explore unlikely connections between well known milestones in technology, tech culture, and seemingly mundane things and events that helped bring them into being. The importance of these seemingly insignificant sparks could not have been imagined at the time of their introduction. The discussion starts with the story of how the Casio mini calculator led directly to the formation of the software giant Microsoft. Next, the talk will explore how early 1970s minicomputer field techs accidentally invented the first personal microcomputers, predating the Altair, IMSAI, and Apple I. The conversation will move to the hidden connections between Datapoint computer company CEO Harold O'Kelley, the Intel 4004 processor, and the eventual dominance of the Ethernet networking protocol over token ring and ARCnet. The presentation will conclude with a story of unlikely connections between a 1963 hearse, the Commodore 64 version of the *Ghostbusters!* software package, and the true uncredited originator of the story that the film and game was based on.
Saturday 1100 Serpico

The Hidden World of Game Hacking

Nick Cano

A common misconception in the world of online gaming is the idea that the only game you can play is the one in the title. Contrary to this, game hackers find enjoyment playing the game that hides behind the curtain: a cat-and-mouse game of wits between game hackers and game developers. While game hackers work to reverse engineer game binaries, automate aspects of game play, and modify gaming environments, game developers combat the hacker-designed tools using anti-reversing techniques, bot detection algorithms, and heuristic data-mining. This talk highlights the fight put up by game hackers, and the advanced methods they have engineered to manipulate games while simultaneously eluding game developers in the dark corners of their own software.
Saturday 2100 Serpico

How to Prevent Security Afterthought Syndrome

Sarah Zatko

Outside of the hacker community, security as an afterthought has always been the norm. Too often we see the following: systems designed without thought for security, then later that system is compromised, and finally a hastily created patch is released (if we're lucky). But did you know that this "security as an afterthought" approach is what we currently teach in schools? Yes, even many of the best schools teach and treat security as a separate topic, leaving it for an advanced class that interested seniors or graduate students might choose to take as an elective. It is all too easy for an undergraduate student to gain a computer science degree without ever learning about the security concepts relevant to their specialty. Security is an integral facet of just about every topic in computer science. Rather than treating security as an afterthought, something that we address after all the foundations are fully in place, it should be treated as an integral part of networking, programming languages, operating systems, and just about every other computer science discipline. Especially offensive aspects! Fixing the way we teach security is a tall order, but it's a more lasting solution. Most short term solutions are Band-Aids on the root problem. Perhaps most encouragingly, we have an existence proof of security being successfully integrated in other fields. This talk will cover computer science curricula, how security is taught and integrated throughout course work in academia, and evaluate an exemplar in a different science where security is being integrated in early curriculum.
Friday 2200 Serpico

HTTP Must Die

Yan Zhu, Parker Higgins

We all know that HTTP is insecure, but the Snowden revelations of 2013 showed that insecurity runs far, far deeper than most of us could have imagined. It's bad enough, in fact, that anyone who still supports it is contributing to the weaponization of the Internet by government spy agencies. The speakers believe that nobody at HOPE X has any excuse to be using plain HTTP instead of HTTPS in 2014. In this talk, they will summarize what the Snowden revelations mean for protecting data in transit: scary stuff like how supposedly secure cookies on social network sites can be turned into custom beacons for marking victims of targeted malware. They'll talk about what every web service provider needs to do at the very minimum to mitigate these attacks, and what clients can do to protect themselves. Finally, they will share some success stories from the last year that show how Edward Snowden has raised the bar for web security and created a safer online landscape for the average user.

Friday 1700 Serpico

I Am The Cavalry: Lessons Learned Fuzzing the Chain of Influence

Geoff Shively, Beau Woods, Jen Ellis, Andrea Matwyshyn

I Am The Cavalry is a relatively new grassroots organization with volunteers from around the world, focused on issues where computer security intersects public safety and human life. Their mission is to ensure that these technologies are worthy of the trust we place in them. Manufacturers of medical devices, automobiles, home electronics, and public infrastructure have been quickly adopting computing technologies. Our dependence on computer technology is increasing faster than our ability to safeguard ourselves. Our technology has advanced to the point where we no longer have to ask "can we?" but we rarely ask "should we?" The hope is to fix this through education, outreach, and research. Hear lessons learned from fuzzing the chain of influence, getting root in the C-Suite, escaping echo chamber sandboxing, initiating two-way handshakes, and building human protocol-aware processes, etc.

Friday 2200 Olson

Identifying Back Doors, Attack Points, and Surveillance Mechanisms in iOS Devices

Jonathan Zdziarski

The iOS operating system has long been a subject of interest among the forensics and law enforcement communities. With a large base of interest among consumers, it has become the target of many hackers and criminals alike, with many celebrity thefts of data raising awareness of personal privacy. Recent revelations exposed the use (or abuse) of operating system features in the surveillance of targeted individuals by the NSA, of whom some subjects appear to be American citizens. This talk identifies the most probable techniques that were used, based on the descriptions provided by the media, as well as today's possible techniques that could be exploited in the future, based on what may be back doors, bypass switches, general weaknesses, or surveillance mechanisms intended for enterprise use in current release versions of iOS. More importantly, several services and mechanisms will be identified that can be abused by a government agency or malicious party to extract intelligence on a subject, including services that may, in fact, be back doors introduced by the manufacturer. A number of techniques will also be examined in order to harden the operating system against attempted espionage, including counter-forensics techniques.

Friday 1600 Olson

The Internet Society Speaks - The History, Futures, and Alternate Directions of the Internet and Its Governance

Jeremy Pesner, David Solomonoff, Avri Doria

In 1992, TCP/IP co-inventors Vint Cerf and Robert Kahn founded the Internet Society, instilling their belief that "the Internet is for everyone" into the policies and operations that the institution has championed ever since. The Internet Society has become the de-facto organization that maintains attention and lobbies on behalf of the public interest on all issues of Internet policy. Thanks to SOPA, Snowden, and the recent FCC rulings, issues of Internet policy are now very much in the public eye, but certain details have been misunderstood or misrepresented in the frenzy of discussion and reports. This talk by members and employees of the Internet Society will help to inform and educate HOPE attendees, providing them a solid knowledge base and history of Internet policy to work from. The three panelists each maintain different areas of expertise within the field of Internet studies: Jeremy has researched and written on the early history of the Internet's development and the policies discussed by the Clinton administration that brought the technology into everyday use; David has long been active in grassroots Internet efforts and can speak to some of the less traditional perspectives on Internet governance; Avri will speak to the worldwide governance efforts and the deliberations around the Internet among several countries. The panel will examine the history of the Internet, the policies around it and some of the key initiatives it has helped to spark.

Friday 1800 Serpico

Jumping the Carbon-Silicon Boundary for Fun and (Mostly) Profit

Tom Keenan

Kevin Warwick made history in 1998 with an RFID chip implanted under his skin. He went on to use sophisticated electrodes to control a robotic arm, achieved human to human nervous system hookups, and even tried transatlantic teledildonics with his wife. Fast forward to 2014 as eager consumers strap on wearable fitness monitors and allow Samsung's creepy eye icon to track their gaze, just so their video will pause when they look away. Worried about Google learning your habits from your Nest thermostat? Your Nike+ FuelBand probably knows a lot more about you, like those times you burned 150 calories at 3 am without taking a single step. Japan's smart toilets realize you're getting sick before you do, and they can tell your doctor. Or, perhaps, your insurance company. This talk presents some of the most intriguing privacy-invading body technologies and looks forward warily to the near future, when the skin cells you leave on a store's PIN pad might be DNA sequenced without your knowledge. You won't believe how many people are after your body-data, and how much it's going to be worth on the open market. There are things you can do to protect your bio-privacy, but you have to start now!

Sunday 1800 Serpico

Keeping Old Code Alive: The Venerable LambdaMOO Server in 2014

Todd Sundsted

The LambdaMOO server, the application server that still powers the LambdaMOO online community and that was the engine for hundreds of other text-based virtual worlds (MUDs), was first released over 20 years ago, in 1991. MUDs (Multi-User Dungeons) were the first networked virtual worlds; and they were popular long before Second Life, Word of Warcraft, and MMORPGs in general made their appearance. Even though much of the code in the current LambdaMOO server is unchanged from the early 90s, people today still download the code, compile it, and build little worlds with it. Motivated by a desire to build simple little immersive experiments that users could interact with and extend via programming, but frustrated by LambdaMOO's lack of features as well as source code that was several decades away from modern best practices, Todd spent the last four years modernizing the server, and building applications and a library of application building blocks. The result is a fork of the codebase called Stunt that speaks HTTP (instead of telnet), includes up-to-date cryptographic primitives, and sports language enhancements like multiple inheritance and garbage-collected, anonymous objects. On top of this platform, he built a simple, modern MVC web framework. In the process, he learned quite a bit about maintaining, evolving, and extending old code, and about interacting with a small but passionate community of longtime users! Sharing these learnings, rather than talking about the specific technical details, is the purpose of the presentation.

Sunday 1000 Olson

Keynote Address - Daniel Ellsberg

We're thrilled that the whistleblower of all whistleblowers - Daniel Ellsberg - will be one of our keynote speakers this year. Ellsberg was the cause of one of the biggest political controversies ever seen in the United States when he released the Pentagon Papers in 1971 and changed history. We are honored that Daniel Ellsberg recognizes the value and importance of the HOPE X conference and it's great to know that he'll be able to speak in person to a whole new generation of individuals who will also shape the direction of the world one day. We can only hope they'll also be ready to stand up for their convictions, no matter the cost.

Saturday 1300 Manning, Serpico, Olson

Lessons Learned from Implementing Real Life Whistleblowing Platforms

Jurre van Bergen, Sacha van Geffen

Whistleblowers and online whistleblowing platforms have received quite a bit of attention recently. Discussions range from the feasibility of implementing a sufficiently secure platform online for whistleblowers, to the changing role of journalism, to the ethics of whistleblowing itself. The lessons learned from implementing multiple whistleblowing platforms in various contexts will be presented here. The main experience is from Publeaks, a Dutch whistleblowing system based on the GlobaLeaks platform, launched in September of 2013. (Publeaks now has almost all of the national press on board.) The development of other leaking sites - like Wildleaks in Africa - will be discussed. Globaleaks and SecureDrop will be introduced and compared. The panel will reflect on social and legal challenges that your group might be facing if you try to implement a whistleblowing platform. You will get some practical and theoretical insight into how you can create your own platform, whether for internal whistleblowing in an organization or for broad multi-stakeholder installations like Publeaks.

Sunday 1000 Manning

Lockpicking, a Primer

Jos Weyers

If you're curious about what lockpicking is all about, this is the talk for you. Several different ways of opening a lock will be shown (picking, bumping, snapping, key impressioning) and explained in detail. No prior lockpick experience or knowledge is needed. This talk will start at ground level. Lockpicking has a clear analogy with the digital world (you have a firewall, therefore you are secure; it has a lock, therefore it must be safe). Consider that physical access will, in lots of cases, render your digital security measures obsolete. After this talk, expect to start rethinking your physical security.

Friday 1500 Manning

The Many Faces of LockSport

Deviant Ollam, Jos Weyers, Doug Farre, JGor, Ray

In the past decade, the hacker subculture of LockSport has seen a tremendous explosion. What was once the purview of dedicated specialists, far-flung hobbyists, and college students meeting in secret is now featured prominently at technical conferences, family-oriented science fairs, and even TV shows. The Open Organisation Of Lockpickers now has nearly 20 chapters across the Netherlands, the United States, and Canada. Sportsfreunden der Sperrtechnik is still going strong with hundreds of members. Locksport International has meetup groups in major cities. Regional groups like the Fraternal Order Of LockSport, the Longhorn Lockpicking Club, the FALE Association of Locksport Enthusiasts, and more conduct local meetings and engage in joint ventures with larger organizations. At the annual LockCon conference, sport pickers from over a dozen countries gather to learn from one another and compete head to head. Despite the shared interest and community between all LockSport groups, there is great variation between the cultures and values of these participants. This panel discussion will feature some of the key figures from various locksport organizations around the world and will hopefully highlight some of those differences and offer the audience a chance to ask questions about locks, LockSport, and competitive lock-opening.

(A primer on basic lock-picking and lock-opening techniques will be offered very quickly at the start of the session if you've never learned these kinds of skills before!)

Friday 1600 Manning (2 hours)

Media, Popular Misconceptions, and the CSI Effect - What Does It Mean for InfoSec and Tech Policy?

Sandy Clark (Mouse), Joshua Marpet

Forensics is tedious and occasionally mind numbing. Exploit discovery and development is extremely detail oriented, and requires strong coding skills. Good Blue Team defensive strategy and implementation is team based, precise, and careful. But put a white lab coat on and, apparently, it's all magic! From Abby's "It's commercial encryption, so it's <dramatic pause> Cracked!" to CSI's famous, "Enhance! Magnify!

Enhance!," the tropes of the popular entertainment world follow Arthur C. Clarke's famous saying" "Sufficiently advanced technology is indistinguishable from magic." So let's make all techs wizards! How does this popular view of tech wizardry help our hacker world? How does it hurt us, when we have to enter the courtroom, either as an expert witness, or as a defendant? How can you, when put into one of these <slightly uncomfortable> situations, defuse these tropes and make them work for you, or at least not hurt you? Does this distorted world view hurt or help technical people, companies, organizations, and agencies, in the world of tech policy, governmental regulations, and National Security Letters? Let's talk.
Friday 1100 Manning

Movie: *Algorithm*

A feature-length movie about computer hackers directed by Jonathan Schiefer

Running time: 91 minutes

"The geeks have inherited the earth... the rest of you just don't know it yet." In San Francisco, nine months before Edward Snowden leaked documents that prove the NSA spies on everyone, Will, a freelance computer hacker, specializes in breaking into secure systems. During a job, he stumbles across a way into Emergent See, a top-secret government contractor. Will downloads all of their recently developed software, including the conspicuously named Shepherd. Every time Will attempts to access Shepherd, bad things happen, starting with his apartment burning down, kidnapping, etc. Will makes it his mission to break into Shepherd and find out why someone is willing to go to such extremes to keep it secret.

Free vegan popcorn supplied by director Jonathan Schiefer, who will be on hand after the screening for a question and answer session followed by movie prize giveaways.
Saturday 2359 Manning

Movie: *Die Gstettensaga: The Rise of Echsenfriedl*

A science fiction and fantasy comedy film directed by Johannes Grenzfurthner and starring Sophia Grabner, Lukas Tagwerker, and Jeff Ricketts

Running time: 72 minutes. Languages: English and German (with subtitles)

The growing tension between the last two remaining superpowers - China and Google - escalates in the early 21st century, and results in the global inferno of the "Google Wars." But the years go by, radioactive dust settles on old battlegrounds, and a new world rises from the ashes of the old. Fratt Aigner, a seedy journalist, and Alalia Grundschober, a nerdy technician, live and work in Mega City Schwechat: the biggest semi-urban sprawl in the foothills of what remained of the Alps. Newspaper mogul Thurnher von Pjölk assigns them a special task: to venture into the boondocks of the Gstetten and find the legendary Echsenfriedl. It is the beginning of a journey full of dangers, creatures, and precarious working conditions. The film was co-produced by art tech group monochrom and the media collective Traum and Wahnsinn, and created for the Austrian television channel ORF III.
Friday 2359 Manning

Movie: *The Internet's Own Boy: The Story of Aaron Swartz*

A documentary directed by Brian Knappenberger

Running time: 105 minutes

The story of programming prodigy and information activist Aaron Swartz. From Swartz's help in the development of the basic Internet protocol RSS to his co-founding of Reddit, his fingerprints are all over the Internet. But it was Aaron's groundbreaking work in social justice and political organizing, combined with his aggressive approach to information access that ensnared him in a two-year legal nightmare. It was a battle that ended with the taking of his own life at the age of 26. Aaron's story touched a nerve with people far beyond the online communities in which he was a celebrity. This film is a personal story about what we lose when we are tone deaf about technology and its relationship to our civil liberties.

Director Brian Knappenberger will be in attendance for a question and answer session after the screening.
Saturday 2200 Manning

Movie: *War on Whistleblowers: Free Press and the National Security State*

A documentary directed by Robert Greenwald

Running time: 67 minutes

This hacker-relevant film highlights four cases where whistleblowers noticed government wrongdoing and took to the media to expose the fraud and abuse - only to be prosecuted and persecuted. Features interviews with no less than three HOPE X speakers (Thomas Drake, Daniel Ellsberg, and Jesselyn Radack), along with many others known to the hacker community.
Friday 2359 Serpico

North Korea - Using Social Engineering and Concealed Electronic Devices to Gather Information in the World's Most Restrictive Nation

Mark Fahey

North Korea prevents its citizens from accessing any form of independent media or information. Any citizen who attempts to access foreign broadcasts to seek information from the outside world risks being interned in one of the state's notorious prison camps. The very few visitors allowed into the country are strictly forbidden to bring any radios, GPS receivers, or other communications equipment. As a result, little independent and objective information about the propaganda-based mass media of the country has been gathered and published. Over four successive trips into each province of the DPRK, Mark has smuggled electronic equipment in and out to capture, monitor, record, and analyze hundreds of hours of local and regional domestic radio and television broadcasts used by the North Korean regime as a prime instrument of control over the population. This will be a fast-paced interactive audio/visual presentation of rare video, audio, and still photography together with an explanation of the social engineering techniques he used to successfully travel throughout North Korea and covertly gather information with concealed electronic equipment.
Sunday 1600 Manning

Obfuscation and its Discontents: DIY Privacy from Card Swap to Browser Hack

Daniel C. Howe

Data collection, aggregation, and mining have dramatically changed the nature of contemporary surveillance. Refusal is not a practical option, as data collection is an inherent condition of many essential societal

transactions. In this talk, we discuss one response to this type of everyday surveillance, a tactic called obfuscation. Tactical obfuscation can be defined as the strategy of producing misleading, false, or ambiguous data with the intention of confusing and/or inhibiting an adversary. Because obfuscation is relatively flexible in its use by average citizens as well as by experts, it holds promise as a strategy for DIY privacy and security. This talk presents a brief overview of obfuscation as political theory, including contemporary and historical examples, then focuses on two recent systems that address data collection: TrackMeNot, which shields searchers from surveillance and data profiling, and AdNauseam, which targets advertising networks that track users across the web. The talk concludes with a consideration of the ethics of obfuscation as representative of a class of strategies whereby weaker parties can both protect against and confront stronger adversaries.
Friday 1200 Olson

Per Speculum In Ænigmate

Maximus Clarke

In the fall of 2013, artist Maximus Clarke was inspired by news of government and corporate surveillance to create an art project about privacy that could also function as a secure messaging system. The result is "Per Speculum in Ænigmate" - Latin for "through a glass darkly" - combining stereo imagery and PGP encryption. Each project image is an anaglyph 3D photo of a nude model, obscured by pixelation and overlaid with an encrypted message sent by one of the project participants. Message recipients are able to download images from the project site (http://psiae.tumblr.com) and decrypt the embedded texts, without the artist ever reading them. This presentation will showcase the project images in glorious old-school red/blue 3D (glasses will be provided), and discuss the concepts, technologies, and processes involved in their creation.
Friday 1700 Olson

Postprivacy: A New Approach to Thinking about Life in the Digital Sphere

tante

The social construct of privacy is rather new, a result of the civil society. It was supposed to protect people from the state and/or government and its overreach, a "right to be let alone," as one of the central legal texts defined it. Privacy promised a safe space for the individual to develop new ideas without premature criticism and discrimination, a space where individual freedom unfolded. Did it really deliver on that promise? And was that the promise we needed as a society? Privacy isn't dead as some people might want to tell you, but it has changed significantly in its definition, in its relevance. And it no longer works as the central foundation of our social utopias. Private people are alone, powerless, and often invisible when faced with exactly those powerful entities that the Internet was supposed to help us fight (corporations, government agencies, etc.). Under the blanket term #postprivacy, some people have started developing ideas on how to rethink how we can harness not only the power of the Internet but the powers, ideas, and skills of each other. How will we as a social structure work between social networks, government snooping, and encryption? How can we save and form the future? This talk will give you a few new ideas.
Friday 1900 Olson

PRISM-Proof Email: Why Email Is Insecure and How We Are Fixing It

Phillip Hallam-Baker

We have had the technology to make email secure against criminals and government spies for decades. Microsoft, Netscape, and Apple have all shipped products with built-in encryption for over 15 years, yet almost nobody uses these features. Millions of people were very upset by the recent Snowden revelations - why aren't millions of people using secure email and, more importantly, how do we fix it? A part of the reason for the lack of email security is rooted in politics. During the 1990s, cryptography rights activists battled with the NSA and FBI for the right to use strong cryptography, a series of events known as the cryptowars. One part of the problem is that two email security standards emerged rather than one, neither of which is capable of fully replacing the other. But the biggest part of the problem is that any system which requires the user to be thinking about security is too hard to use. This talk will be looking at the history and future of email encryption technology. No prior knowledge of cryptography will be assumed.
Sunday 1400 Manning

Privacy-Friendly Hypertext? Do Not Track, Privacy Badger, and the Advertising-Funded Web

Peter Eckersley

This talk will introduce the design and implementation of Privacy Badger, EFF's new browser extension that automatically blocks both invisible trackers and spying ads. It is intended to be a minimal- or zero-configuration option that most Internet users can use to prevent nonconsensual third party collection of their reading habits from their everyday browser. Privacy Badger couples the recently developed HTTP Do Not Track opt-out header with a number of heuristics for classifying the behavior of third parties to automatically determine which should be blocked, which are needed but should have cookies blocked, and which are safe from a privacy perspective. Peter will also talk about the bigger picture on the role that nonconsensual commercial surveillance has come to play in the business and technical infrastructure of the Web; and what we can do to build better alternatives.
Sunday 1800 Manning

Project PM: Crowdsourcing Research of the Cyber-Intelligence Complex

Andrew Blake, Gregg Housh, Kevin Gallagher, Joe Fionda, Douglas Lucas

In April 2013, the FBI sought information on what the journalist Barrett Brown was doing with an open source collaborative wiki that he founded called Project PM, and were equally as curious about what kind of dirt he had on his hard drives about the government contractors and intelligence firms he investigated on that site. Edward Snowden's leaks about the NSA have since exposed only the tip of the iceberg with regards to how much the U.S. intelligence community is capable of, and those efforts are largely assisted by the likes of companies who Project PM set out to research: Ntrepid, Abraxis Hacking Team, Cubic, Endgame, Palantir, and others. Now, more than ever, is the time to collect and analyze open source information about the shadowy companies who operate on behalf of the U.S. government, often without being held accountable.
Saturday 1600 Serpico

#radBIOS: Yelling a Database across the Room

Richo Healey

How can you distribute digital information using only sounds and computers? Frustrated by the lack of compatibility of wireless hardware in the wild, it was concluded that the audible spectrum was the One True Way to distribute knowledge. This talk will introduce Groundstation, an append-only graph database, and detail the journey of integrating it with the unambiguous encapsulation research of Ossmann/Spill to achieve its ultimate goal - the audible sharing of digital knowledge.

Saturday 1000 Olson

The Repair Movement

Sandra Goldmark, Michael Banta, Vincent Lai, Miriam Dym, Tiffany Strauchs Rad

Mending (or fixing/repairing) - part of the spectrum that includes hacking, alteration, and making - can become a political act in a time of cheap goods, outsourced labor, and low wages. What is mending's role in a new model of production and consumption, one where artisans and individuals face off, perhaps quixotically, against mass production? Can repair become economically viable? How does mending contend with goods that are poorly made in the first place, when globalization undermines local resources, when companies design objects *and* supply chains to be repair-resistant? Panelists from the repair movement will discuss the opportunities as well as the barriers to making repairs in the human realm: social (habits and systems), economic (prices, labor), and technical (parts, design). Repairing things, rather than discarding or putting up with broken objects or systems, connects deeply to the hacker/maker movement and to sustainable ecology. Panelists will address how repair can be beautiful as well as potentially disruptive. This panel includes activists and artists, attorneys and organizers - drawn to repair as process and performance. An act of repair has the possibility of political significance or an act of resistance, and brings the possibility of transformation to ordinary objects and larger systems alike.

Friday 1000 Manning

Reverse Engineering - Unlocking the Locks

Matthew O'Gorman aka mog

If you can't tear it apart, drive it, or modify it, do you really own it? This talk seeks to free a Kwikset PowerBolt and show you how to reverse engineer and take back control of your life. The Kwikset PowerBolt lock has support for a Z-Wave module. You will learn how to diagram the function of all the ICs on the Z-Wave daughter board and the Kwikset main board, how the interfaces are used across the board, how the components are connected to each other, how to spy on the traffic, and finally how to replace the Z-Wave module with your own daughter board created in gEDA. This knowledge will give you the freedom to lock and unlock your front door in any way you can imagine. This talk will teach you how to use a multimeter to test for continuity and voltage, a bus pirate to quickly test protocols, logic analyzer tools to sniff traffic on the board, and other electrical tools. You will learn how to diagram a system at the flow chart and schematic level and best practices on how to learn a system.

Saturday 1800 Olson

Rickrolling Your Neighbors with Google Chromecast

Dan "AltF4" Petro

Take control over your neighbors' TVs like in the movies! The Google Chromecast is a handy little gadget that lets you stream video to your TV from a variety of sources like Netflix and YouTube. It also happens to allow streaming from nearby hackers. This talk will demonstrate how to hijack any Google Chromecast - even if it's behind a secure Wi-Fi network - to do your bidding. A new tool will also be released to fully automate the hijacking and playing of arbitrary video to the victim's TV. Let the prank war commence.

Friday 2100 Serpico

The Science of Surveillance

Jonathan Mayer

The National Security Agency is bound by legal constraints. It hasn't always followed the rules, to be sure. But when it does, are constitutional and statutory safeguards effective in protecting our privacy? This talk presents empirical computer science research on the NSA's legal restrictions, including results cited by President Obama's intelligence review group. We find that present limits on bulk surveillance programs come up far short. Authorities intercept international Internet traffic and enable the monitoring of ordinary Americans' online activities. The domestic telephone metadata program reaches much of the population, and allows for drawing extraordinarily sensitive inferences about medical conditions, firearm ownership, and more.

Sunday 1300 Olson

Screening: *Rambam Gets His Man*

The world premiere of the Investigation Discovery (ID) TV series, based on incidents surrounding the FBI arrest of Steve Rambam at HOPE Number Six. It all took place at the Hotel Pennsylvania, shortly before his panel covering how to track down an evasive person. (His talk was rescheduled by HOPE staff four months later at Stevens University to a standing-room-only audience.) Charges were later dropped, then refiled by DOJ, then dropped again. The lead FBI Special Agent on case was later arrested on 20 felony fraud counts.

This world premiere will be followed by a question and answer session featuring Steve Rambam and some of the people behind the series.

Saturday 1200 Serpico

A Sea of Parts

Per Sjoborg

Have you heard of Self Re-Configuring Modular Robotics (SRCMR)? This new technology enables robotic modules to configure themselves into whatever you need, whenever you need it, which offers many benefits. If we could create a common pool that modules can be drawn from when they are needed and returned to when they are not, we could further leverage the benefits of SRCMR. The challenge is that the pool is not intrinsic to an SRCMR system; we need to create it. We need a new understanding of our common resources and an acceptance for sharing them. If we can create the pool or "a sea of parts," it will bring the same benefits to physical systems that shared web hosting has brought to the web. This will allow quick and cheap development and deployment of new ideas.

Saturday 2000 Olson

SecureDrop: A WikiLeaks in Every Newsroom

William Budington, Garrett Robinson, Yan Zhu

SecureDrop is an open-source whistleblower submission system that media organizations can use to securely accept documents from and communicate with anonymous sources. The platform has been deployed and is being actively used by an array of journalistic organizations to provide a secure and usable platform for whistleblowers to get in touch with journalists while protecting their own identity. The talk will begin with a broad overview of the project and then go into more detail: what does the network architecture look like, what does it provide, and what cryptographic primitives are used?

Saturday 1200 Manning

Securing a Home Router

Michael Horowitz

Routers sit between all your computing devices and the Internet, making them a perfect target for abuse (Glenn Greenwald has written about the NSA hacking into them). The presentation will explain some of the configuration options in home routers that can make your Local Area Network more secure. Among these are locking down access to the router, Wi-Fi security, firewalls, DNS, and hiding on the Internet. Also covered are known security flaws in routers and how to defend against them. Some of the covered flaws are: WPS, UPnP, port 32764, Heartbleed, and smartphones leaking Wi-Fi passwords.

Sunday 1500 Olson

The Sex Geek as Culture Hacker

Kristen Stubbs

"Being a nerd is not about what you love; it's about how you love it." Wil Wheaton's words ring true for many self-identified geeks and nerds. But what happens when what you love is "love," or even "lust?" Geeks have never been more cool, but mainstream culture is full of negative messages about sex and pleasure. Combining nerd enthusiasm and geek know-how with erotic experiences results in writings, DIY toys, citizen science, and other projects which can promote sex-positivity and consent culture. In this talk, Kristen "where did this b!tch get her doctorate" Stubbs shares stories from the sex geek trenches: the awesome, the awkward, and the randomness in between.

Saturday 2200 Serpico

Shortwave Pirate Radio and Oddities of the Spectrum

Andrew Yoder

Radio has become marginalized and governments are curtailing international shortwave broadcasting, yet these bands remain one of the most anonymous and inexpensive ways to convey information within and across international borders. This presentation will include background information about shortwave radio, its range, what types of stations are on the air (broadcast, military, weather fax, spy numbers, amateur, and more), and finally pirate radio. It will include background information behind pirate broadcasting stations on the air, how stations attempt to maximize their signal quality and range while avoiding detection by the authorities. Some of these tactics have ranged from transmitting from ships, to leaving battery-powered transmitters on public lands, to installing equipment at highway billboards. In an age when IP addresses, GPS, and cell phones track people as well as data, pirate radio is one of the few means of sending untracked, anonymous information.

Friday 1300 Olson

Showing Keys in Public - What Could Possibly Go Wrong?

Jos Weyers

If a reporter wants to get the point across that certain people shouldn't have access to a particular key, would it be wise for said reporter to then show that key to the world? Like the New York City subway key? *The* key to the subway? On the Internet?! This and other media fails will be shown. And maybe even one or two non-fail examples.... Several cases of key-copying-by-sight will be discussed with lots of pictures and videos. How this can happen will be explained, as well as what to do to prevent it.

Saturday 2000 Serpico

Skeuomorphic Steganography

Joshua Fried

Skeuomorphic steganography is spawned in the terrain where art, code, and digital media interbreed. Steganography is the ancient art, revitalized in the digital age, of hiding messages in plain sight. Skeuomorphism is the use of design elements that include features inherent to an earlier design, for example, images of leather binding in on-screen calendars, or faux wood grain printed on vinyl tiles. This talk puts forth the theory that steganography finds a natural home inside skeuomorphism. Sometimes, when one is looking for hidden data, one has to know where to look. This is especially true outside the digital realm. An idea for a new convention will be proposed: Let's have skeuomorphism show us where to look. Joshua will show how printed skeuomorphic steganography can be decoded with simple tools. The dream is of a world, just slightly more fun than this one, in which skeuomorphism takes on a new life, not as kitsch, an eyesore, or some wigged-out aberration at Apple Inc., but as a hint of a possible invitation, a bread crumb left by a new friend.

Saturday 1700 Olson

Social Engineering

Emmanuel Goldstein and friends

The tenth incarnation of this panel, which officially makes it a tradition. One of our biggest draws, this session always delivers something memorable. The panel will tell stories of the magic of social engineering, predict what may or may not be possible in the future, and make a few live attempts over the phone to gain information they have absolutely no right to possess. Sometimes it works and sometimes it fails horribly, as is the very nature of social engineering. You'll learn how to recover from being denied or busted and how to push forward, gaining tiny bits of information until you possess more knowledge about your target than you (or they) ever thought possible.

Saturday 2100 Manning, Olson

Solve the Hard Problem

Gillian "Gus" Andrews

The biases run deep: from early in our school careers, we're taught that "smart people" go into math, science, and tech. There's an unspoken hierarchy many of us have drilled into our heads, with particle physics at the top of the academic food chain, engineering lower down but still higher than that weird

squishy stuff in biology and the even squishier stuff in sociology, etc. "Smart people" tackle the "hard" problems, and the hard problems involve a lot of math, "hard" science, and empirical evidence. Well listen, J. Random Hacker, if you're so goddamn smart, why haven't you built a tool that makes it easy for people to encrypt their email yet? Why is adoption the major barrier to secure communications? Why haven't the tools you've built evened out the digital divide? Is the hard problem infrastructure scaling or the Traveling Salesman problem, or is the really hard problem dealing with the people you could never get to understand what you're doing? This talk will be an exhortation for hackers to overcome the traditional biases many of us have in favor of technical projects and against human-factors work. It's a call for more people to think about usability in open source software, particularly on the privacy and security tools we care so much about. Gus will tease apart the deep-seated socialization we have about what work "smart" people do, what "good" science looks like, and why studies of human social interactions must have different criteria than "hard" sciences in order to be effective.
Friday 1100 Serpico

Spy Improv: Ask Me Anything

Robert Steele

The former spy, honorary hacker, former candidate for the Reform Party presidential nomination, and #1 Amazon reviewer for nonfiction, again takes on any question. His record, set in 2010, is eight hours and one minute. This year, the formal program provides for two hours.
Saturday 2300 Serpico

SSL++: Tales of Transport-Layer Security at Twitter

@jimio

You've enabled HTTPS on your site. Now what? How do you protect against sslstrip attacks, CA compromise, and the dangers of mixed content? @jimio will share some approaches they've taken @twitter: Strict-Transport-Security, "secure SEO" with canonical link elements, Content Security Policy, and certificate pinning. There will be code, exploits, and open source! There will be a few fun stories to share as well, and since this is an SSL talk, you *know* there's gonna be heartbleed.
Friday 2000 Manning

Steepest Dissent: Small Scale Digital Fabrication

Nadya Peek

High precision in fabrication is often required for building useful hardware and tools - including hardware and tools that can be used for dissent. Craftsmanship is valued for its precision and attention to detail, but mastering a craft is inherently slow. 3D printers evoke a *Star Trek* replicator-esque, hands-off solution for instantly creating precise tools, but in that image also become a transparent technology. However, digital fabrication technology as it exists today is anything but transparent, as digital fabrication tools are difficult to access, interface with, modify, and even use as intended. In a way, lack of access to precision fabrication is in itself a form of control. This talk will be about how digital fabrication enables personal fabrication, and how we are getting closer to being able to truly use digital fabrication in technologies for dissent.
Friday 1400 Olson

A Story of Self Publishing Success

John Huntington

Just days before HOPE Number Nine, John Huntington released a self-published version of his book, *Show Networks and Control Systems*. Several months before, his publisher had decided that they were not interested in an update after three successful editions, so Huntington got his publishing rights back and did a whole new edition himself using Amazon's Createspace for printed copies and Kindle for e-books. And it's been a success - Huntington has made far more money self publishing this one edition than the royalties on all three of the previous editions with the publisher combined. More importantly, he has had a far higher level of engagement with his readers, and has been able to do things he never could have done with the publisher, like putting free lecture videos for each chapter on his website, or giving copies away (which he will do at the end of this talk). Huntington will share sales figures, compare the economics and issues related to both printed and e-book editions, and lay out the challenges, pitfalls, and successes of this process.
Sunday 1600 Olson

Stupid Whitehat Tricks

Sam Bowne

How can you improve security at companies that haven't hired you or given you permission to test their systems? Non-intrusive methods such as Google searches and observing headers can detect some serious problems without trespassing on networks. Sam found problems at thousands of websites, including dozens of companies and big-name colleges that are currently under hostile control. These problems included SQL injections, website redirectors, Wordpress pingback exploits, and more. Many of the systems were being used by criminals to perform attacks. He notified the companies. Most ignored the notifications. Some of them fixed the problems, a few complained, and one made a serious effort to silence him. In this talk, Sam will show how he found the problems, how he notified the administrators, and how they reacted. Whitehatting can be useful and rewarding, as long as you have realistic expectations and a thick skin.
Sunday 1700 Serpico

Surveillance, Sousveillance, and Anti-Surveillance: Artistic Responses to Watching

Gregg Horton

It's impossible to imagine a world without surveillance. Its presence reflects a symbiotic relationship with the State and hegemony as a whole. For years, artists have been using surveillance and surveillance technologies to engage and disrupt the surveillance apparatus. This talk will explore works by artists such as Steven Mann, Banksy, The Surveillance Camera Players, and many more working in the medium to answer the question of "how are we to engage with a surveillance society?"
Friday 1100 Olson

Teaching Electronic Privacy and Civil Liberties to Government

Greg Conti

Privacy advocates and government officials are often at odds. Ironically, both groups want the same thing - a safe and free democracy. This will be an exploration of how government employees can better make protection of privacy and civil liberties part of

the calculus considered when making security decisions - not just due to legal compliance constraints or fear of a backlash from privacy advocates, but due to a true appreciation that privacy and civil liberties are as important to democracy as is security. This talk will cover initial successes in exposing government employees to electronic privacy and civil liberties material in the classroom, and sketch the outlines of open source training materials. The ultimate objective is to inform and inspire government employees worldwide to propagate legal reform inside the system without taking extreme approaches. The presentation will be interactive, so please come with ideas for content and educational strategies that might be used to educate government employees at all levels and in a wide variety of countries on the importance of electronic privacy and civil liberties.
Sunday 1200 Serpico

There's No API for Dying

Nathan Bennett

"There's No API for Dying" inspires hackers to think more creatively about users by examining the role of death in hardware and software development. Traditionally, Human Computer Interaction has been about using a user-centered design process to create products that ultimately do not require humans to adapt or change to use these products derived from the user-centered design process. The reality is that many products have left behind this process as they have forgotten, failed, or never felt the need to design for the death of a user. Hackers are encouraged to explore an alternative thanatosensitive design process that mandates designers account for the death of a user in their hardware and software projects because death is a part of the user's experience.
Sunday 1400 Olson

This Is the X You Are Looking For

Eric (XlogicX) Davisson, Ruben Alejandro (chap0)

When you hear you are being profiled for which books you check out in a library, what do you do with this knowledge? Do you tell your friends to "evade," to not check these books out, or to find other means of getting this content? No. You tell everyone in the world to deliberately check these books out (and now we have had the pleasure of reading *Catcher in the Rye*). This talk is about looking signature detection in the face and confusing or saturating the tool or analyst. A number of techniques will be explored, including a fun malware signature trick called a tumor (it's OK, it's benign), and others focusing on open source Intrusion Detection Systems. There may be some random banter about grocery loyalty cards, too. Although this talk intends to be just as technical as expected at a conference like this, it will also be light, fun, and philosophical in nature. Expect a gratuitous slide deck, lots of terminal action, signatures in the nude, hex, and beautiful regex.
Saturday 1000 Serpico

Threat Modeling and Security Test Planning

Eleanor Saitta

How do I figure out if the application I've designed is secure? What do I need to test? When do I need to start thinking about security? How does what an application is designed to do affect how it's tested? How do high-level security goals relate to protocol bugs? How do I know when I need specialist review? How do I figure out if my users will be able to use my application securely? If you've found yourself asking questions like these or if you're just realizing that maybe you should be asking them, this talk will give you tools to work with. The work that a security analyst does can be opaque, but understanding it will save you time and help you build a more secure application. This talk will cover threat modeling (both on its own and as a driver of high-level test planning), when and which kinds of low-level tests you should be including, with special attention paid to parser/protocol bugs. Examples will be shown from both the commercial space and the world of software designed for high-risk users, with specific focus on some of the particular challenges of the latter arena.
Saturday 1100 Olson

Thwarting the Peasants: A Guided and Rambunctious Tour Through the *2600* DeCSS Legal Files

Jason Scott

In 2000, a whole lot of movie companies sued a whole lot of people over the coding of a routine called DeCSS, which would allow the access and playback of DVDs in Linux and any other platform that felt the burning desire to watch Hollywood movies. The full name of the court case has a name too long for this description, but by the time it was over, a whole host of individuals had dropped out, leaving *2600 Magazine* and the rest fighting over the point of whether linking to infringing materials is itself infringement. The case was decided in Hollywood's favor, and passed into the realm of history. A decade later, the extensive files related to this case were slated for disposal, and Jason Scott volunteered to take possession of them. These files are now being scanned in, and contain all manner of amazing material, some highlights of which will be shown in this presentation. The case was a time capsule of an industry expecting yet another rolling over of the populace as to who truly owned the media. It didn't quite work out that way. Expect a level of excitement not usually found in court transcripts and evidence collections.
Saturday 1600 Manning

Travel Hacking with The Telecom Informer

TProphet

When people talk to TProphet (also known as The Telecom Informer) about how he travels and lives all over the world, experiencing destinations from Armenia to Antarctica, they often say something like "I could never afford that!" If you think like a hacker, though, travel doesn't have to be expensive. You will learn how tickets for an around-the-world trip were booked for under $219, and how you can also travel for little or nothing. The world is an incredible place to explore. This talk will encourage you to get out and see it!
Sunday 1400 Serpico

Unmasking a CIA Criminal

Ray Nowosielski

"Her name is Alfreda Frances Bikowsky." While those six words may seem innocuous, according to the Central Intelligence Agency, if made publicly, they might have sent Ray and his journalist colleagues to prison. On September 8, 2011, they received the first in a series of phone calls and emails from CIA's media rep Preston Golson. "We strongly believe it is a potential violation of federal criminal law [the IIPA Intelligence

Identities Protection Act] to print the names of two reported undercover CIA officers whom you claim have been involved in the hunt against al Qa'ida." They had used this approach successfully several times in the past to persuade some of America's most respected journalists - Jane Mayer of *The New Yorker*, Adam Goldman and Matt Apuzzo of the Associated Press, among others - to withhold her name from the public. Seeking advice from the ACLU's National Security Project, its lead attorney Ben Wizner made them aware that she had become something of an open secret in his world. They had stumbled onto a hornet's nest. Bikowsky, as it turned out, was the person credited internally with the greatest PR coup of the Obama White House, the successful assassination earlier that year of Osama bin Laden. As chief of the Global Jihad Unit, she reportedly runs the nation's drone strikes program. She is a through-line running from the failure to prevent 9/11 to the push for war in Iraq to the development of the CIA's renditions, black sites, and torture program and continuing to today's targeted assassinations in countries around the world. Through her story, we can see the details of a devolution in the rule of law and the justice system in America, as well as the impetus for and birth of what some call the "war on whistleblowers and journalists." For 20 years, she has been at the center of history, yet the covert nature of her job has prevented that history from ever before being told to the public in one place. Doing so is necessary for a democratic citizenry to have an informed discussion about national security and intelligence policy in America's continuing fight against terrorism.

Friday 2200 Manning

Updates from the Online Identity Battlefield

aestetix, Kaliya IdentityWoman

At HOPE Number Nine, aestetix gave a general introduction to the world of nyms (short for pseudonym) and NymRights (the group he created to promote online self-expression). Things have changed a lot in the last two years. More services are moving online, and there are a lot of discussions about how to securely "verify" users, how to prevent fraud/harm, and how to do all of this while keeping our civil liberties intact. There have also been developments with the National Strategy for Trusted Identities in Cyberspace (NSTIC), an Obama strategy designed to promote these discussions in places like health care and social security. The White House is finalizing points on their Cybersecurity Framework (which includes NSTIC) and, in the meantime, a bunch of web services are implementing "verification" solutions, some with better success than others. In light of fundamental "nym" ethics, the discussion will take a look at these strategies and solutions, show which work better than others and why, and introduce some things the panelists have been working on as well.

Saturday 2300 Olson

Usable Crypto: New Progress in Web Cryptography

Nadim Kobeissi

This talk will provide an outline of the pitfalls, dangers, benefits, and progress when it comes to doing encryption in JavaScript in the browser. Nadim has been working on this problem for the past three years in collaboration with Mozilla, Google, and the W3C. The solution is still far away, but there have been many interesting (and, most importantly, educational) challenges that have been faced. After giving an overview of how browser cryptography has advanced in the past year, Nadim will reveal a new open source encryption software project during the talk.

Saturday 1500 Olson

Using Travel Routers to Hide in Safety

Ryan Lackey, Marc Rogers

In light of the past year's NSA revelations and the long history of SIGINT, safe network use is a serious concern, especially for international travelers. Open source and commercial tools to hide one's identity when traveling will be described here, in the face of both blanket surveillance and targeted, intense monitoring. You will learn about tools which can be comfortably taken through restrictive border regimes and carried openly in war zones without attracting undue attention - as would suit a journalist or human rights worker. While these tools tend to be complex, the true challenge is the threat model: a single slip-up, undetected at the time, can doom the user and the user's contacts to discovery, interrogation, or worse.

Friday 2300 Manning

Vigilante Justice: Masks, Guns, and Networks

Zimmer Barnes

This talk will cover the state of vigilante action around the world; what they fight with, who their targets are, how they stay anonymous, and how they organize. Without condemning or condoning any single act, these radically unique responses to crime and corruption deserve our attention. How much power are they wielding? Is nonviolence winning out over violence? Is anonymity giving way to irresponsible action? And what should we expect as these networks deepen? There's a growing list of options being explored, and these explorers have dramatic and largely unknown stories to tell.

Friday 2300 Olson

Visualization for Hackers: Why It's Tricky, and Where to Start

Tamara Munzner

Computer-based visualization systems provide visual representations of datasets designed to help people carry out tasks more effectively. Visualization is suitable when there is a need to augment human capabilities rather than replace people with computational decision-making methods. The design space of possible vis idioms is huge, and includes the considerations of both how to create and how to interact with visual representations. Vis design is full of tradeoffs, and most possibilities in the design space are ineffective for a particular task, so validating the effectiveness of a design is both necessary and difficult. Vis designers must take into account three very different kinds of resource limitations: those of computers, of humans, and of displays. Vis usage can be analyzed in terms of why the user needs it, what data is shown, and how the idiom is designed. Tamara will discuss the implications of all this trickiness for systems visualization, where the datasets include trace logs, network traffic, and semi-structured text in addition to the classic big table of numbers. One good way forward is to think hard about how to transform your original data into a form that's well suited for addressing the user's problems

(CONT'd ON PAGE 22)

FRIDAY

	Manning	Serpico	Olson
1000	The Repair Movement	Are You Ready to SIP the Kool-Aid?	
1100	Media, Popular Misconceptions, and the CSI Effect	Solve the Hard Problem	Surveillance, Sousveillance, and Anti-Surveillance
1200	Barrett Brown and Anonymous: Persecution of Information Activists	A Beautiful Mosaic: How to Use FOIA	Obfuscation and its Discontents: DIY Privacy
1300	When Whistleblowers Are Branded as Spies	Wireless Meshnets: Building the Next Version of the Web	Shortwave Pirate Radio and Oddities of the Spectrum
1400	The Hacker Wars - A Conversation with NSA Whistleblower Thomas Drake	Apophenia: Hunting for the Ghost in the Machine	Steepest Dissent: Small Scale Digital Fabrication
1500	Lockpicking, a Primer	Hacking the Patent System	When Confidentiality and Privacy Conflict
1600	The Many Faces of LockSport	Can You Patent Software?	Identifying Back Doors and Surveillance Mechanisms in iOS
1700		HTTP Must Die	Per Speculum In Ænigmate
1800	Community Owned and Operated Cellular Networks in Rural Mexico	The Internet Society Speaks - Internet and Its Governance	G-code: The Programming Language of Machining and 3D Printers
1900	Building an Open Source Cellular Network at Burning Man	Why the Future is Open Wireless	Postprivacy: Life in the Digital Sphere
2000	SSL++: Tales of Transport-Layer Security at Twitter	Art under Mass Surveillance	Ergonomic Human Interface Hacking
2100	Dark Mail	Rickrolling Your Neighbors with Google Chromecast	Crypto for Makers
2200	Unmasking a CIA Criminal	How to Prevent Security Afterthought Syndrome	I Am The Cavalry: Fuzzing the Chain of Influence
2300	Using Travel Routers to Hide in Safety	The Web Strikes Back - Fighting Mass Surveillance	Vigilante Justice: Masks, Guns, and Networks
2359	Movie: *Die Gstettensaga: The Rise of Echsenfriedl*	Movie: *War on Whistleblowers: Free Press and the National Security State*	

SATURDAY

	Manning	Serpico	Olson
1000	Bless the Cops and Keep Them Far from Us	This Is the X You Are Looking For	#radBIOS: Yelling a Database across the Room
1100	Ask the EFF - This Year on the Internet	Hearses and Hand-Held Calculators: Unlikely Connections	Threat Modeling and Security Test Planning
1200	SecureDrop: A WikiLeaks in Every Newsroom	Screening: *Rambam Gets His Man*	Visualization for Hackers: Why It's Tricky
1300	Keynote Address - Daniel Ellsberg	Keynote Address - Daniel Ellsberg	Keynote Address - Daniel Ellsberg
1400	A Conversation with Edward Snowden	A Conversation with Edward Snowden	A Conversation with Edward Snowden
1500	Disruptive Wearable Technology	(Geo)location, Location, Location: Mobile Location Surveillance	Usable Crypto: New Progress in Web Cryptography
1600	Thwarting the Peasants: The *2600* DeCSS Legal Files	Project PM: Crowdsourcing Research	Your Right to Whisper: LEAP Encryption Access Project
1700	You've Lost Privacy, Now They're Taking Anonymity	Electric Waste Orchestra	Skeuomorphic Steganography
1800		Hacking Money, from Alexander the Great to Zerocoin	Reverse Engineering - Unlocking the Locks
1900		When You Are the Adversary	DIY Usability Research
2000	Biohacking and DIYbiology North of the 45th Parallel	Showing Keys in Public - What Could Possibly Go Wrong?	A Sea of Parts
2100	Social Engineering	The Hidden World of Game Hacking	Social Engineering
2200	Movie: *The Internet's Own Boy: The Story of Aaron Swartz*	The Sex Geek as Culture Hacker	Codesigning Countersurveillance
2300		Spy Improv: Ask Me Anything	Updates from the Online Identity Battlefield
2359	Movie: *Algorithm*		

SUNDAY

	Manning	Serpico	Olson
1000	Lessons Learned from Real Life Whistleblowing Platforms	Cyber Security in Humanitarian Projects	Keeping Old Code Alive
1100	Ethical Questions and Best Practices for Service Providers	Bringing Down the Biological System	Will It Blend? How Evil Software Clogs the Pipes
1200	Elevator Hacking: From the Pit to the Penthouse	Teaching Electronic Privacy to Government	Bootkits: Step-by-Step
1300		Fuckhackerfucks! An Audience Bashing	The Science of Surveillance
1400	PRISM-Proof Email	Travel Hacking with The Telecom Informer	There's No API for Dying
1500	Cultures of Open Source	Drop It Like It's Hot: Secure Sharing for Journalists	Securing a Home Router
1600	North Korea - Using Social Engineering	Community Infrastructure for FOSS Projects	A Story of Self Publishing Success
1700	Blinding The Surveillance State	Stupid Whitehat Tricks	Echoes of Returns Lost: The History of The Telecom Digest
1800	Privacy-Friendly Hypertext?	Jumping the Carbon-Silicon Boundary	
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: x.hope.net/codeofconduct.html

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.

before you dive into the details of exactly how to draw any pictures.
Saturday 1200 Olson

The Web Strikes Back - Fighting Mass Surveillance with Open Standards
Harry Halpin

After the Snowden disclosures, it was revealed that the NSA and NIST were subverting the open standards process by intentionally weakening the security of the core standards that form the foundation of the web and Internet. Now, more than ever, we need cryptographically strong standards and verified open source libraries for these standards. The humble origins of the IETF and the W3C will be discussed, as will the efforts taken by open standards to combat pervasive surveillance via workshops like STRINT and the "perpass" mailing list, and the new standardization work that is likely to result. In particular, the focus will be on the myriad problems implicit in putting cryptography into the web security model with the W3C Web Cryptography API, as well as attempts to analyze properties of this JavaScript API by using techniques from formal proof-proving. There's also new work from the W3C on decentralized social networking - and all the security problems that entails! Most importantly, you'll learn how you can get involved to help build open standards to build what Tim Berners-Lee calls the "Web We Want" - and stop the web from being subverted.
Friday 2300 Serpico

When Confidentiality and Privacy Conflict
Daniel Kahn Gillmor

We have many mechanisms to provide confidential communications so that network operators and other would-be surveillance regimes can't inspect the content of our traffic. But some of those mechanisms actually reveal more about who is speaking than cleartext communication would, especially over longer periods of time and large datasets. Information about who is speaking to whom is so valuable that large organizations devote huge amounts of resources to assembling network graphs of this "metadata," even without the content of the communications. Clearly this information is worth something; it is probably worth protecting. Why should privacy (hiding who you are) conflict with confidentiality (hiding what is being said)? This talk will look at specific instances of privacy and confidentiality conflicts, and describe patterns that create this tension. There will also be a discussion on some approaches to resolve the conflict and outline ways to improve privacy while preserving confidentiality.
Friday 1500 Olson

When You Are the Adversary
Quinn Norton

If your name isn't Barton Gellman, Laura Poitras, or Glenn Greenwald, chances are that while the NSA may be a rights-violating threat to all, it's not your actual, day-to-day adversary. Real world adversaries tend to be spouses, parents, bosses, school administrators, random drive-by malware, and maybe local law enforcement. While federal threats create a terrible security culture, they aren't stepping into the lives of most people. And while obsessing over various intelligence agencies and trying to build tools against them makes you feel like a badass, it doesn't help most people. Fixing Flash and building easy to use communication tools does change the lives of countless people. This talk will focus on the infosec needs of the 99 percent - who aren't geeks. This talk will touch upon the value of bad crypto when it lets someone escape an abusive spouse, and the common situations where tools that let people sidestep the requirements of their IT departments make the world a better place. Yes, the big bad guys still matter, but fighting a billion little bad guys probably matters more.
Saturday 1900 Serpico

When Whistleblowers Are Branded as Spies: Edward Snowden, Surveillance, and Espionage
Jesselyn Radack

When *The Guardian* and *Washington Post* published the first stories exposing the National Security Agency's surveillance operations based on revelations from the whistleblower Edward Snowden, the world learned that U.S. government officials told a series of misleading half-truths and outright lies to conceal what has become a U.S. surveillance industrial complex. The revelations revealed massive waste, fraud, abuse, illegality, and an equally massive loss of valuable intelligence. In response to the understandable public outrage about their mass surveillance, the NSA chose not to investigate the officials who needlessly and in secret sacrificed the privacy of hundreds of millions of innocent people. Rather, the intelligence community has spent untold resources investigating and attempting to discredit Snowden. It is a predicable response for an institution to focus on the messenger rather than the message. It can be an effective distraction to focus the media and public attention on one individual rather on exposing systematic, widespread illegality in a powerful government agency. Whistleblowers in all corporate and government spheres risk choosing their conscience over their careers, but under the Obama administration, national security and intelligence whistleblowers face choosing their conscience over their very freedom. The Obama administration has prosecuted more people under the Espionage Act for alleged mishandling of classified information than all past presidential administrations combined. The Espionage Act is an arcane, vague, and overbroad World War I-era law intended to go after spies, not whistleblowers. NSA whistleblower Thomas Drake objected to mass surveillance using internal channels and was charged under the Espionage Act. Central Intelligence Agency whistleblower John Kiriakou objected to torture and was charged under the Espionage Act. He is now serving 30 months in prison. Army Private Chelsea Manning helped expose war crimes and is serving 35 years after facing Espionage Act charges. Because of this pattern of persecution, Edward Snowden was forced to leave the United States and seek asylum in Russia after the U.S. government left him stranded in the Moscow airport last year. This talk, by a member of Snowden's legal team, will address all of this and more.
Friday 1300 Manning

Why the Future is Open Wireless
Adi Kamdar, **Nate Cardozo**, **Ranga Krishnan**

How do we begin the movement to create a world

of ubiquitous open wireless, where sharing and openness is the norm? How do we get it to spread? Speakers from EFF's activism, legal, and technology teams will describe the open wireless movement (https://www.openwireless.org) and the specific challenges their open wireless router campaign is solving. The first hurdle is convincing the world that sharing Wi-Fi with guest users is, as security expert Bruce Schneier puts it, a matter of "basic politeness." Another perceived roadblock is the belief that running an open network could subject the host to legal liability. Lastly, even proponents of open wireless lack easy technical solutions to safely enable private and anonymous guest access without reservations. To that end, EFF is developing an easy to set up, secure Wi-Fi router. But, in order to truly realize our open wireless future, they will need your help.
Friday 1900 Serpico

Will It Blend? How Evil Software Clogs the Pipes
Michael Sikorski

During an investigation, Michael discovered an attacker who was emailing himself from an infected user's account. He sent and received emails under the radar via Outlook extension malware. Countless times Michael has seen attackers forced to blend their malware communications with the noise on his clients' networks. The talk will start with a brief history lesson on malware and its use of the network for command-and-control and data theft. Then there will be some fun opening his malware vault to explore interesting specimens from the wild such as the Outlook Assistant and malware that tweets! The presentation will close by discussing how you can find and analyze malware that communicates on the network and why traditional network monitoring isn't enough - attackers will find a way out of your network no matter how small a funnel you put them through.
Sunday 1100 Olson

Wireless Meshnets: Building the Next Version of the Web
Kevin Carter, Peter Valdez, Kurt Snieckus

This panel will feature discussion and debate about the exciting current state of wireless meshnet technology, with a particular focus on how to build and join local urban wireless networks separate from the traditional Internet. A short tutorial of the project as well as how to connect to a local meshnet - including an overview of the necessary open hardware and software required - will be provided at the beginning of the panel. After the tutorial, a discussion will occur regarding the scope and impact of the global meshnet project. Technology covered will include the CJDNS project, Hyperboria, installing the Meshberry image on a Raspberry Pi device, configuring Ubiquiti NanoStation M5 routers featuring the OpenWrt software, and other relevant topics. Whether you're a new user or an enthusiast, this is a great place to learn more about the technology driving new free and secure private networks.
Friday 1300 Serpico

Your Right to Whisper: LEAP Encryption Access Project
Micah Anderson

The LEAP Encryption Access Project is dedicated to giving all Internet users access to secure communication. Their focus is on adapting encryption technology to make it easy to use and widely available. Like free speech, the right to whisper is a necessary precondition for a free society. Without it, civil society languishes and political freedoms are curtailed. As the importance of digital communication for civic participation increases, so too does the importance of the ability to digitally whisper. When you attempt to secure your communications online, you are faced with confusing software, a dearth of secure service providers, and involuntary leakage of critical information. For aspiring service providers, barriers to entry include the high cost and technical complexity of setting up secure servers. LEAP's goal is to transform secure online communication from an exercise in frustration into an automated and straightforward process for those whose access to information and free expression depend upon confidentiality, authenticity, and the protection of their social networks. Come to this talk to hear about LEAP's unique strategic infrastructure approach taking federated standards and open protocols to tackle these problems and find out how you can too. Also, there will be pretty pictures of birds.
Saturday 1600 Olson

You've Lost Privacy, Now They're Taking Anonymity (aka Whistleblowing is Dead - Get Over It)
Steve Rambam

Government and private entities are working to shred privacy and warehouse personal, relationship, and communications data. Once unimaginable surveillance technologies are being perfected and implemented. The most intimate details of lives are routinely and unthinkingly surrendered to data-gatherers. Is it still possible to be an anonymous whistleblower? Is it still possible to be anonymous at all? Your physical location and activities for the past ten years are known and have been logged. If you attend a church or synagogue or mosque or a demonstration or visit an abortion clinic or a "known criminal activity location" or meet with a "targeted person" or a disliked political activist, it is routinely recorded. Your finances, sexual orientation, religion, politics, habits, hobbies, and information on your friends and family are gathered, indexed, and analyzed. Facial recognition, camera analytics, license plate readers, and advances in biometrics allow you to be de-anonymized and remotely surveilled 24/7/365 by machines. Forensic linguistics, browser and machine fingerprinting, and backdoors substantially eliminate the possibility of anonymous Internet activity. Thanks to "The Internet of Things," your thermostat and electric meter report when you arrive home and your garbage can reports when you throw out evidence to be collected by the few remaining human agents. "Predictive profiling" even knows what you will do and where you will go in the future, so the data collection bots can be waiting for you. Data collection now begins at birth. And no data gathered will ever be thrown away. And none of the data gathered belongs to you or will be under your control ever again. An internationally-known private investigator and long-time HOPE speaker, Steve will describe in frightening detail how the last shreds of everyone's anonymity are being ripped away. Real world examples will be used. Surprises can be expected.
Saturday 1700 Manning (3 hours)

SPEAKERS

aestetix, after being suspended twice from Google Plus during nymwars, helped co-found NymRights, focused on preserving identity freedom on the Internet. For verification's sake, he was also involved when the Knights Templar overtook the Spanish Armada, and has secret documents from the NSA about the aliens.

Ruben Alejandro (chap0) started with an associates in computer science and did the networking gig for a while. He then toyed around in a variety of security operations, policy, and vulnerability positions while taking on CCNA security, CEH, GPEN, and OSCP in the process. His interests are in the offensive side of security. He is a contributor to Metasploit and has submitted a few exploits to exploitdb, ranging in various platforms and attack types. He's contributed and developed CTF scenarios for P.L.U.G. in Phoenix and has been a member of the Corlan team for some time now. He has also written for *2600*.

Micah Anderson is an activist who has been experimenting with technology to use it to create grassroots technology alternatives like riseup.net, Indymedia, Debian, and the LEAP project.

Gillian "Gus" Andrews' peculiar career has been forged in the fires of HOPE, attending since 2002, speaking since 2006, and organizing since 2010. This has helped her into such fine messes as a doctorate on how people do and don't use web addresses to navigate online, a brief stint as a panelist on the radio show *Off The Hook*, interviewing Mitch Altman with puppets on her web series *The Media Show*, and her current position as the lead of Secure User Practices at the Open Internet Tools Project.

Michael Banta is the cofounder of Pop Up Repair, an itinerant repair service for household items of all kinds. The project has appeared in New York City storefronts and farmers' markets, and has sparked a strong response.

Zimmer Barnes views the world through the lens of being raised by an antigovernment activist and has spent several years in the vigilante underground. He has been involved with multiple vigilante operations and has observed, aided, and led a wide variety of missions. He has been featured on *Wired's* "Danger Room" blog, as well as the HBO documentary *Superheroes*. Zimmer also helped provide security and medical aid during the Occupy Wall Street protests in Zuccotti Park.

Nathan Bennett is a software developer by day who researches and studies Human Computer Interaction, end-of-life care, and assistive technology by night. Nathan graduated from the University of North Carolina at Asheville with a degree in Multimedia Arts and Science. He enjoys web development, hacking hardware, and is passionate about information security, having worked for law firms and in network administration.

Andrew Blake is a journalist who has worked closely on issues concerning Anonymous and hacktivism for a number of outlets. He's appeared on RT and HuffPost Live to discuss computer crimes and the intelligence sector, and covered the case of WikiLeaks source Chelsea Manning for vice.com.

Matt Blaze is a hacker, safecracker, and computer science professor at the University of Pennsylvania, where he studies surveillance, security, cryptography, and large-scale systems.

Peter Bloom is a member of Rhizomatica (rhizomatica.org) and a community digital defense and autonomy advocate and scholar who lives in Oaxaca, Mexico.

Sam Bowne has been teaching computer networking and security classes at CCSF since 2000. He has given talks at Defcon, BayThreat, LayerOne, Toorcon, and lightning talks at HOPE. He has a CISSP and a PhD and a lot of computers and cables and firewalls and stuff.

Willow Brugh is the director of Geeks Without Bounds, an accelerator for humanitarian projects. Previous endeavors include being co-founder of Seattle makerspace Jigsaw Renaissance, the hackerspace collaboration initiative Space Federation, and the response-development competition GameSave. Years of participation in the hacker and makerspace community have created purpose towards distributed systems, engaged citizens, and mutual aid. With heavy involvement in Maker Faire, Random Hacks of Kindness, and the SpaceApps Challenge, Willow's main skill is "getting out of the way."

Finn Brunton is an assistant professor in media, culture, and communication at NYU Steinhardt. He is the author of *Spam: A Shadow History of the Internet* (MIT Press, 2013), *Obfuscation: A User's Guide* (with Helen Nissenbaum, forthcoming MIT 2015), and is researching a book on digital cash and cryptocurrencies.

William Budington is a web application architect at the EFF, and one of the core developers of SecureDrop, an anonymous document submission platform. He is a member of the W3C Web Cryptography Working Group, and is excited to see the web grow as a platform for cryptographic applications.

Nick Cano is a 21-year-old software enthusiast who has been making, breaking, hacking, and fixing software since the age of 12. He spends his weekdays working as a senior security engineer at Bromium, his weekends authoring a game hacking book for No Starch Press, and his nights developing and selling a bot for an online game.

Nate Cardozo is a staff attorney on the Electronic Frontier Foundation's digital civil liberties team. In addition to his focus on free speech and privacy litigation, Nate works on EFF's "Coders' Rights" project and "Who Has Your Back?" report. A 2009-2010 EFF Open Government Legal Fellow, Nate spent two years in private practice before returning to his senses and to EFF in 2012. Nate has a B.A. in anthropology and politics fromU.C. Santa Cruzand a J.D. from U.C. Hastings where he has taught first-year legal writing and moot court. He brews his own beer, has been to India three times, and watches too much Bollywood.

Kevin Carter is a technologist, writer, and musician whose work has been featured at HOPE and Skytalks (Defcon 21). He has published work in *2600*, *The Fiction Circus*, and *Kerouac's Dog Magazine*, and he is the host of a monthly multimedia literary reading in New York City called "Derangement of the Senses."

Kevin Chen is from Ottawa and is currently a masters student in McGill's bionanomachines program. His background in synthetic biology and DIYbio comes from leading award-winning teams in the iGEM (International Genetically Engineered Machine) competition while at Queen's University, and he also explores new ways of doing and sharing science while working for Synbiota, an online platform for collaborative and open science research.

Richard Cheshire, known as The Cheshire Catalyst since his days of publishing the *TAP Newsletter* in the 1970s and 80s, is now retired in Florida where he has his very own area code (321), and watches satellites launch from the Canaveral Spaceport. He wants to share the Asterisk open source OS with the phreak community.

Sandy Clark (Mouse) has been taking things apart since the age of two, and still hasn't learned to put them back together. She is a security researcher and Ph.D. candidate at the University of Pennsylvania. Her research focuses on understanding the mechanisms driving the computer security arms race and in modeling the cyber-security ecosystem. A founding member of TOOOL-USA, she also enjoys infrastructure hacking and exploring the myriad fascinating and unexpected ways that systems interact.

Maximus Clarke (http://maximusclarke.com) is a multimedia artist who lives and works in Brooklyn, NY. His stereographic and video works have been featured in exhibitions at the Warhol Museum, the Clocktower Gallery, the Center for Holographic Arts, Radiator Gallery, Devotion Gallery, and elsewhere. He also creates electronic music, videos, and performances under the name Maxx Klaxon (http://klaxon.tv).

Gabriella Coleman is an author and professor. Trained as an anthropologist, she holds the Wolfe Chair in Scientific and Technological Literacy at McGill University. Her research, teaching, and writing covers the ethics and politics of digital activism and computer hackers. Her first book, *Coding Freedom: The Ethics and Aesthetics of Hacking*, has been published with Princeton University Press, and her new book with Verso, *Hacker, Hoaxer, Whistleblower, Spy: The Story of Anonymous*, will be out in November, 2014.

Greg Conti is an associate professor at West Point. He is the author of *Security Data Visualization* (No Starch Press) and *Googling Security* (Addison-Wesley), as well as over 60 articles and papers covering online privacy, usable security, security data visualization, and cyber warfare. He has spoken at numerous academic and hacker forums. His work can be found at www.gregconti.com.

Sasha Costanza-Chock is a scholar, activist, and mediamaker who works in the areas of social movement communication, community-led design, and media justice. He is Assistant Professor of Civic Media at MIT's Comparative Media Studies/Writing, and is a faculty affiliate at the Center for Civic Media, the MIT Open Documentary Lab, and the Berkman Center for Internet and Society. He cofounded VozMob, leads the Vojo team, and sits on the board of Allied Media Projects.

Josh Datko is the founder of Cryptotronix, LLC (www.cryptotronix.com), an open source hardware startup. He is also a submarine and Afghanistan veteran, and graduate of the U.S. Naval Academy.

Eric (XlogicX) Davisson has obtained degrees in computer engineering, business, and criminal justice. He's recently obtained SANS certifications like GCIH and GCIA (incident handling and intrusion analyst, respectively), but he's no crime fighting businessman superhero with the superpower of alphabet soup trailing his name. He uses all of this knowledge in trade and for lulz. His interest is in the obscure. His favorite languages are assembly and Perl (because it treats regular expressions with the respect they deserve). Eric has been active in his local Phoenix *2600* community for well over a decade.

Bill Degnan is a former lecturer of computer history at the University of Delaware. He currently runs the classic computing blog web site vintagecomputer.net and he is a veteran speaker for HOPE and other events related to computing and technology. Bill's writings and photography have appeared in *Wired*, BBC radio, and CNN online. He is currently working on a documentary about computer collecting.

Alessandro Delfanti is a postdoctoral fellow at McGill University in Montreal and the author of *Biohackers: The Politics of Open Science*.

Connor Dickie is cofounder and CEO of Synbiota.

Johnny Diggz is an entrepreneur, musician, filmmaker, and founder of Geeks Without Bounds. In 1995, he co-founded IRDG (Intergalactic Research and Development Group), which built the world's first Internet-based unified messaging platform, iPost. In 1999, he co-founded Voxeo Corporation and serves as chief evangelist for Voxeo Labs' flagship cloud communications platform, Tropo, and its community of over 250,000 developers. He produced the indie feature film, *The Karaoke King,* a musical comedy that premiered in 2007 at the Cinema City International Film Festival. Johnny is also a professional dueling piano player and will perform at the slightest arm-twist.

Avri Doria has been involved with the Internet Corporation for Assigned Names and Numbers (ICANN) and the Generic Names Supporting Organization (GNSO) since 2005. She is the first winner of the ICANN Multistakeholder Ethos Award.

Thomas Drake is a decorated U.S. Air Force and U.S. Navy veteran, and was a senior executive and technical director for NSA's software engineering and implementation - where he discovered and blew the whistle on massive multi-billion dollar fraud, waste, and abuse; the failures that led to 9/11; and the widespread violations of citizens' rights through secret mass surveillance programs after 9/11. After years of addressing these issues in vain thorough official channels, Drake finally went to the press - and soon became the first whistleblower since Daniel Ellsberg in 1971 to be charged with espionage. He faced spending the rest of his life in federal prison for defending the Constitution. After refusing to testify against his colleagues and demanding a jury trial, the government's case of all ten felony counts collapsed in 2011 and he went free. Drake is the recipient of the 2011 Ridenhour Truth Telling Prize, a joint recipient with Jesselyn Radack of the 2011 Sam Adams Associates Integrity in Intelligence Award, and the 2012 Hugh M. Hefner First Amendment Award. He has been keenly interested in the many developments within the hacker world over the years.

Gaston Draque is a VoIP development and deployment specialist at Nexacomm, an IP telephony supplier. He is also a Digium certified Asterisk professional and is involved in the future of telephone switching technology via Internet Protocol.

Charles Duan is the director of the Patent Reform Project at Public Knowledge, a DC-based nonprofit organization that promotes the public interest in technology policy and supports strong patent reform that minimizes the impact of patent trolls and other abuses of the patent system that get in the way of new technologies. He works closely with lawmakers in Congress, the White House, the U.S. Patent and Trademark Office, and other places, to ensure that patent law promotes innovation rather than overreaching and impeding technologists. He previously practiced as a patent attorney and also was a software developer at a Silicon Valley startup.

Miriam Dym is founder of Logo Removal Service and other disruptive art-business ventures. She has shown at museums and galleries in the U.S. and abroad, including the Brooklyn Museum of Art and SFMOMA. She has held residencies at The Watermill (Long Island, New York), Cite des Arts (Paris), and Stanford University Digital Art Center.

Peter Eckersley is technology projects director for the Electronic Frontier Foundation. He keeps his eyes peeled for technologies that, by accident or design, pose a risk to computer users' freedoms - and then looks for ways to fix them. He explains gadgets to lawyers, and lawyers to gadgets. Peter's work at EFF has included privacy and security projects such as Panopticlick, HTTPS Everywhere, SSDI, and the SSL Observatory; helping to launch a movement for open wireless networks; fighting to keep modern computing platforms open; and running the first controlled tests to confirm that Comcast was using forged reset packets to interfere with P2P protocols. He holds a PhD in computer science and law from the University of Melbourne. His research focused on the practicality and desirability of using alternative compensation systems to legalize P2P file sharing and similar distribution tools, while still paying authors and artists for their work.

Jen Ellis is senior director of public and community affairs for Rapid7.

Daniel Ellsberg was the cause of one of the biggest political controversies in the history of the United States when he released the Pentagon Papers in 1971. This top-secret Pentagon study of U.S. government decision-making concerning the Vietnam War was released to various newspapers. When the *New York Times* was stopped by a Nixon administration court order, Ellsberg leaked the 7,000 pages of documents to the *Washington Post* and 17 other publications. These revelations clearly showed deceptive practices by the government and played a significant role in changing the views of many Americans - and ultimately in changing history. When Ellsberg turned himself in to face trial for his actions, he said, "I felt that as an American citizen, as a responsible citizen, I could no longer cooperate in concealing this information from the American public. I did this clearly at my own jeopardy and I am prepared to answer to all the consequences of this decision." After a trial which revealed massive corruption and various nefarious plots against Ellsberg, all charges were dismissed.

Mark Fahey lives in Sydney, Australia and is a health informatics specialist who develops clinical solutions. His other current projects include Satdirectory (a free-to-air satellite directory), and MediaExplorer, a virtual travel guide to webcams and free-to-air digital satellite reception of information about remote lands and intriguing cultures.

Doug Farre is the president of Locksport International, a recreational organization focused on promoting and fostering the hands-on, interactive, and stimulating hobby of picking locks. Doug is interested in all types of security and has written, advocated, and spoken on the subject for years. Additionally, he has acted as a physical security consultant for numerous institutions. He currently lives in Boulder, Colorado and works as a web and mobile applications developer at Quick Left Inc.

Todd Fernandez is a hacker, a mechanical engineer, and a perpetual student. He also builds large 3D printers. His experience and interest in G-code does not originally come from 3D printers, but from the world of CNC milling machines. He is currently pursuing a PhD in engineering education and teaches classes on machining for fun.

Joe Fionda is a data intersectionality and privacy enthusiast who works as an actor, producer, and journalist. He is in the upcoming documentary called *The Hacker Wars*, premiering at the Toronto Film Fest in September, and has appeared on *Boardwalk Empire*, *Law and Order: SVU*, and *Power*, among others. He is a staunch defender of journalists and the 99 percent in the fight against income inequality.

Joshua Fried is a musician first and a coder second, or third. As composer, performer, and producer his work spans experimental music, DJ culture, and live art. He has remixed They Might Be Giants, drummed on electric shoes, and put headphones on downtown New York City's most mercurial stars. Fried has performed solo at Lincoln Center, The Kitchen, Danceteria, La MaMa, BAM, Joe's Pub, and le Poisson Rouge (all in New York City), as well as in Los Angeles, Miami, Tokyo, Berlin, Milan, Paris, and across Europe. His solo project, RADIO WONDERLAND, turns corporate media into recombinant funk, live in real time, and will perform at HOPE X. He teaches music technology at NYU.

Kevin Gallagher is a systems administrator and activist who is interested in privacy and freedom of information. After Barrett Brown's arrest, he created Free Barrett Brown, a support network, advocacy organization, and legal defense fund. To that end, he has been responsible for much of the public efforts that have been put forth regarding Brown's defense. He now works for Freedom of the Press Foundation.

Eva Galperin is the International Freedom of Expression coordinator at the Electronic Frontier Foundation. She has worked for the EFF in various capacities for the last five years, applying her political science knowledge and technical background to organizing activism campaigns and doing education and outreach on intellectual property, privacy, and security issues. A lifelong geek, Eva misspent her youth working as a systems administrator all over Silicon Valley. Since then, she has seen the error of her ways and earned degrees in political science and international relations from SFSU. She comes to EFF from the U.S.-China Policy Institute, where she researched Chinese energy policy, helped to organize conferences, and attempted to make use of her rudimentary Mandarin skills. Her interests include aerials, rock climbing, opera, and not being paged at three in the morning because the mail server is down.

Barton Gellman is a Pulitzer Prize winning journalist and author, senior fellow at the Century Foundation, and lecturer at Princeton. He is one of three journalists who received classified archives from Edward Snowden. Gellman is leading NSA coverage at *The Washington Post* and writing a book on the surveillance-industrial revolution.

Ahmed Ghappour is a professor at UC Hastings College of the Law. There, he directs a project that addresses constitutional issues in national security and cyber security prosecutions across the country. His scholarship looks at the interplay between emerging technology and national security - particularly as demonstrated by the modern surveillance state and the evolution of cyberspace as a theater of war. Formerly, Ahmed was a diagnostics engineer at SGI's high performance computing division.

Daniel Kahn Gillmor is a technology fellow at the ACLU and a member of the Debian project. When he's not working on network protocols, free software, or civil liberties implications of technology, he's probably cooking or riding his bicycle.

Sandra Goldmark is the cofounder of Pop Up Repair, an itinerant repair service for household items of all kinds. Founded and staffed by theater artists, the project provides an alternative to the cycle of use-and-discard consumer goods.

Emmanuel Goldstein is the editor of *2600*, organizer of the HOPE conferences, and host of WBAI's *Off The Hook* radio program. He never intended for any of this to happen.

Johannes Grenzfurthner is an artist, writer, curator, and director. He is the founder and artistic director of monochrom, an internationally-acting art and theory group. He holds a professorship for art theory and art practice at the University of Applied Sciences in Graz, Austria. He is head of the "Arse Elektronika" sex tech festival in San Francisco, host of "Roboexotica" (Festival for Cocktail-Robotics, Vienna and San Francisco), and just finished his first feature film (*Die Gstettensaga: The Rise of Echsenfriedl*). Recurring topics in Johannes' artistic and textual work are contemporary art, activism, performance, humor, philosophy, postmodernism, media theory, cultural studies, sex tech, popular culture studies, subversion, science fiction, and the debate about copyright and intellectual property.

Carl Haken is a Brooklyn-based developer, DevOps engineer, and entrepreneur. He has a keen interest in human-computer interfaces.

Phillip Hallam-Baker is a member of the original CERN team that designed the World Wide Web. Dr. Hallam-Baker is a leading designer of Internet security protocols. Standards based on his original work have been approved by IETF, W3C, and OASIS and are implemented in virtually every device that connects to the Internet.

Harry Halpin is team contact for the Web Cryptography and Social Web Working Group. He is also president of the board of LEAP (LEAP Encryption Access Project). He supports the freedom to protest, and so has had his laptop seized at the U.S. border and has been detained by FBI agents - and has spoken out on DRM being standardized at the W3C.

Richo Healey is a flat duck enthusiast hailing from Melbourne. In the past he's worked on everything from distributed systems to reverse engineering .Net assemblies, once even sinking so low as to boot a PHP vm inside of a goroutine. Nowadays, he focuses on platform security at Stripe.

Parker Higgins is an activist and blogger at EFF, working to advance policy and technology fixes to online freedom of speech and privacy violations. He was a leader of the San Francisco CryptoParty, and tweets at @xor.

Harlo Holmes is the 2014 Knight Mozilla Open News Fellow at the *New York Times*. She also is a research fellow and Head of Metadata for The Guardian Project (https://guardianproject.info), the open-source mobile security group.

Bill Horne had a career at "Mother Bell" that spanned 25 years. He joined New England Telephone and Telegraph Company as a technician, worked his way up to systems analyst at NYNEX, and was chosen for the SS7 groups at Verizon Engineering during the last part of his Verizon tenure. He was, at various points in his engineering years, in charge of the E911 network in New England, part of the "RFP" team for the Tekelec Eagle STP units employed to enable local number portability, and was also responsible for PC security in the Marlborough, Massachusetts Verizon office. Since accepting an early retirement offer, Bill has run his own business, offering PBX, VoIP, and network services to various customers in the Boston area.

Michael Horowitz has been a computer nerd since 1974 when IBM mainframes were the only computers. He has blogged about defensive computing for many years (defensivecomputing.info) and is currently an independent consultant.

Gregg Horton is a web developer and multimedia artist from Oakland, California who focuses on sound art, Ruby, JavaScript, and Rupture.

Gregg Housh is an activist focused on Internet freedoms, censorship, over-prosecution, and Anonymous. He has appeared on countless news programs and in publications around the world to speak about hacktivism, Anonymous, and Project PM.

Daniel C. Howe is an artist, writer, coder, and critical technologist, whose work focuses on the aesthetic and political implications of computational technologies. He currently lives in Hong Kong.

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

Kaliya IdentityWoman is the co-CEO of the Leola Group based in Oakland, California - a stealth startup focused on creating the decentralized semantic data technology. Prior to this, she founded the Personal Data Ecosystem Consortium (http://www.pde.cc), a network of startups around the world building tools for people to collect, manage, and get value from their personal data. She co-founded and continues to lead the twice a year Internet Identity Workshop (http://www.internetidentityworkshop.com), the world's leading innovation forum for user-centric identity and personal data technologies. She was born and raised in Vancouver, Canada. Her first career was as a water polo player and won a gold medal at the 1999 Pan-American Games.

Colten Jackson is a machine and design assistant at the Champaign Urbana Community Fab Lab in Illinois. Working with a diverse set of fabrication tools and surrounded by a wonderful community of makers, Colten works to introduce people to technologies they might not expect they have access to and creates objects that exemplify what happens when talent pools overlap within the maker movement.

JGor has had a hand in running the Longhorn Lockpicking Club since its inception at the University of Texas at Austin in the fall of 2006. In addition to running the club, he organizes lockpick villages and events for various security conferences. By day he is a network security analyst for the university, where his physical hacking adventures have ranged from defeating locking manhole covers to cracking cryptographic RFID card-access systems.

@jimio works on Twitter's product-security team; he delights in short biographies.

Adi Kamdar is an activist at the Electronic Frontier Foundation specializing in patent, free speech, intermediary liability, andconsumer privacy issues. He also coordinates EFF's open access advocacy and helps with student activism. Adi studied History of Science at Yale University, where he was chapter president and a member of the board of directors of Students for Free Culture. Previously, he interned at EFF, at the Berkman Center for Internet and Society, and with the Open Video Alliance. In his free time, he enjoys improv, music, things that are delicious, and being outdoors.

Tom Keenan learned to program in FORTRAN and assembly language in the 1960s at a secure computer facility in New York City, presumably to help America fight the post-Sputnik Russian menace. Instead, he was often seen around the early *2600* meetings and also playing with pay telephones. He went on to a respectable career as a computer science professor and technology journalist in Canada. He has interviewed interesting people from John Draper (Cap'n Crunch) to Arthur C. Clarke to FBI, NSA and State Department officials. In addition, he co-wrote the award-winning CBC Radio series *Crimes of Future*. He also helped design Canada's first computer crime laws and is a fellow of several prestigious societies. Currently professor of environmental design at the University of Calgary, he is the author of the new book: *Technocreep*.

Brian Knappenberger is a writer, director, and producer who has created award winning investigative documentaries and feature films for *FRONTLINE/World*, *National Geographic*, Bloomberg Television, and PBS. His recent award winning independent feature, *We Are Legion: The Story of the Hacktivists*, explored the online "hacktivist" group Anonymous and chronicled a year of unprecedented online protest activity. Brian's previous films have explored the political tension and corruption behind rebuilding southern Afghanistan in *Life After War* and brutal abuses of power and a violent crackdown on speech in Ukraine in *A Murder in Kyiv*. His newest film, *The Internet's Own Boy: The Story of Aaron Swartz*, premiered at the 2014 Sundance Film Festival (and will be screened at HOPE X).

Nadim Kobeissi, originally from Lebanon, is a programmer and cryptography enthusiast whose work focuses on making encryption more accessible to people around the world. He created Cryptocat, one of the world's most popular encrypted chat solutions and a gold standard for easy-to-use private chat. Nadim is a member of the W3C's web cryptography working group and holds a double degree from Concordia University in Montreal. Currently, he acts as cryptography engineer at eQualitie for their DDoS mitigation platform.

Eric Koeppen is a member of the IBM X-Force Advanced Research Team. After graduating from Texas Tech University, he went to work for the DoD in the field of information security. Later, he left government service to become a contractor working for the Air Force, as well as other DoD customers, still in the InfoSec industry. His main areas of interest are reverse engineering (especially firmware), vulnerability research, and tool development.

Ranga Krishnan is a Technology Fellow at the EFF. He works with the technology projects team to foster development and adoption of technologies that enhance privacy, freedom of expression and access to the Internet. He was formerly a principal engineer in Qualcomm's Office of the Chief Scientist. He is interested in open wireless networks, wireless mesh networks, and redesigning Internet services to enhance user security. Ranga studied electrical engineering at IIT, Madras, then indulged his passion for physics through graduate work at MIT and postdoctoral work at IAS, Princeton, NJ, before returning to the engineering fold.

Ryan Lackey works on security products at CloudFlare, an edge network performance and security company. Previously, he founded HavenCo, the world's first offshore datahaven, and has worked as a defense contractor in Iraq and Afghanistan, and at various startups. He also founded CryptoSeal, a YC funded startup which was sold to CloudFlare in June 2014.

Vincent Lai has been leading the Fixers' Collective, a project-in-residence at the Proteus Gowanus gallery in Brooklyn, since 2010. While he loves to fix and tinker, he's still interested in all opportunities to learn a new and novel way to fix anything. He remembers his first computer, a TRS-80 Model I, and his first HOPE in 2000.

Ladar Levison is the founder of Lavabit, LLC. Founded in 2004 (and originally named Nerdshack), Lavabit served as a place for free private and secure email accounts. By August of 2013, Lavabit had grown to over 410,000 users, with more than 10,000 paid subscribers. He created Lavabit because he believes that privacy is a fundamental, necessary right for a functioning, fair, and free democracy. On August 8, 2013, he made the bold decision to shut down his business after "refusing to become complicit in crimes against the American people." Presently, he is serving as the project manager and lead architect for the Dark Mail Initiative, while continuing to vigorously advocate for the privacy and free speech rights of all Americans.

Wil Lindsay is a hardware hacker, media artist, and educator living in central Pennsylvania. Much of his work revolves around the development of unconventional open-source production tools, used internationally by artists and musicians. Publicly released projects include: oneString, an open-source USB synth controller; the Bliptronome, an open-source port of the Monome controller to a $50 toy; and the YM_MINI, a DIY MIDI synthesizer based on the sound chip from the Atari ST. Information on his exhibitions, performances, and project releases can be found at www.straytechnologies.com.

Douglas Lucas is a freelance writer and journalist whose work covering national security matters, Internet freedom, culture, and more has appeared at *Salon*, *Vice*, *Nerve*, *WhoWhatWhy*, and other venues. He studied philosophy and literature at TCU, graduating summa cum laude. He also enjoys writing fiction, mainly in the SF and fantasy genres.

Joshua Marpet is an adjunct professor at Wilmington University, where he teaches digital forensics, Linux, ethical hacking, and the ethics of information security, among other courses. He has been featured in *Scientific American*, the *Miami Herald*, *Hurriyet News*, *Gizmodo*, *Techcrunch*, EBRU-TV, and many other media outlets. Joshua is an internationally respected digital forensics expert and a former senior information security analyst for the Federal Reserve Bank of Philadelphia. He is also a former police officer from St. Tammany's Parish sheriff's office, and a former volunteer firefighter from New Jersey. In other words, he's done all of his childhood dream jobs except astronaut, and he's working on that!

Andrea Matwyshyn is a senior policy advisor at FTC and a law professor at U Penn Wharton. She advises government agencies on technology and security issues, and has testified before Congress on security legislation.

Jonathan Mayer is a lawyer and a computer scientist. He teaches at Stanford Law School and is a Ph.D. candidate in computer science at Stanford University. Jonathan was named one of the "Forbes 30 Under 30" in 2014 for his work on technology security and privacy. His research and commentary frequently appear in national publications, and he has contributed to federal and state policy making and law enforcement.

Declan McCullagh is the chief political correspondent for CNET. Previously, he was a senior correspondent for CBS News' website, and was for four years the *Wired* bureau chief in Washington, D.C., where he spent over a decade before moving to the San Francisco Bay Area. An award-winning journalist, Declan writes and speaks frequently about technology, law, and politics; his work has appeared in scores of publications including *The Wall Street Journal*, *The New York Times Magazine*, *Playboy Magazine*, *Communications of the ACM*, and the *Harvard Journal of Law and Public Policy*.

!Mediengruppe Bitnik live and work in Zurich/London. Using hacking as an artistic strategy, their works recontextualize the familiar to allow for new readings of established structures and mechanisms. Their works formulate fundamental questions concerning contemporary issues and can be seen at http://wwwwwwwwwwwwwwwwwwwwww.bitnik.org.

Nicholas Merrill is the executive director of The Calyx Institute, a nonprofit organization whose mission is to educate the public about privacy in digital communications and to develop and test building blocks that service providers can use to build "privacy by design" into their service offerings. In a previous career, he was the president of Calyx Internet Access, one of the first ISPs in New York City, founded in 1994. He was the plaintiff in Doe v. Ashcroft - the first legal challenge to the USA PATRIOT Act's National Security Letters provision.

Michael Morisy is the cofounder of MuckRock, a crowdsourced news site that has filed over 8,000 public records requests everywhere from the FBI and NSA to the Wichita Kansas Police Department. Muckrock's investigations have shed light on domestic surveillance techniques, wasteful spending, and how science was rewritten in favor of tough-on-drugs politics.

Aurelia Moser is a 2014 Knight Mozilla Open News Fellow at Ushahidi (http://ushahidi.com) and Internews-Kenya. She toggles between Nairobi and New York working on coding education and open source crisis mapping for journalists.

Alexander Muentz is both a hacker and lawyer. He tries to explain technology to lawyers and law to hackers and techies. You've seen him around at a few other conferences - and when he can't be informative, he can at least be entertaining.

Maka Muñoz is a feminist hacker and anthropologist who works in Mexico to strengthen autonomous communication.

Tamara Munzner is a professor at the University of British Columbia Department of Computer Science and holds a PhD from Stanford. She has been active in visualization research since 1991 and has published over 50 papers and book chapters. She has worked on visualization projects in a broad range of application domains including genomics, evolutionary biology, geometric topology, computational linguistics, large-scale system administration, web log analysis, and journalism.

Kaytee Nesmith is a user experience designer and researcher. By day, she leads mobile UX design for a prominent hospitality company; by night, she helps to make a handful of surveillance circumvention tools easier to use. She enjoys whiskey and syntactically significant whitespace.

Quinn Norton is a writer who likes to hang out in the dead end alleys and rough neighborhood of the Internet. She started studying hackers in 1995, after a wasted youth of Usenet and BBSing. She was *Wired's* correspondent on Anonymous and the Occupy movement in 2011 and 2012. These days, Quinn is a columnist for *Medium* and *MaximumPC*. She covers science, technology, copyright law, robotics, body modification, and medicine, but no matter how many times she tries to leave, she always comes back to hackers.

Ray Nowosielski lives in New York City where he works as a freelance producer for the Emmy nominated series *Vice* on HBO. In 2011, he was greeted with an outpouring of support after the CIA threatened him and his colleagues with prosecution under the Intelligence Identities Protection Act. He had contacted the agency requesting that two of their employees respond to serious allegations which were later detailed in a 90-minute Amazon-only "investigative podcast" entitled *Who is Rich Blee?* An advocate for government and corporate transparency and accountability, he has written for *Salon* and *Truth-Out* and contributed investigations to *The Daily Beast* and *Gawker*.

Bryan Nunez is the project lead for InformaCam at the Guardian Project. Previously, he was the technology manager at Witness, and was a founding advisor for The Engine Room. He is a recognized leader in the strategy and development of online and mobile projects for social change. Throughout his career, he has led the development and product launches of award winning mobile and online projects.

Matthew O'Gorman aka mog is a free software advocate, having contributed to several projects: Asterisk, Erlang, ejabberd, Emacs, PAM, gEDA, etc. He is a free hardware enthusiast who started his own company (Meat Stand) and is a long standing board member of Makers Local 256, a hacker space in Huntsville, Alabama.

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 in his time teaching about lockpicking.

Kurt Opsahl is a senior staff attorney with the Electronic Frontier Foundation, focusing on civil liberties, free speech, and privacy law. He has counseled numerous computer security researchers on their rights to conduct and discuss research. Before joining EFF, Opsahl worked at Perkins Coie, where he represented technology clients with respect to intellectual property, privacy, defamation, and other online liability matters. In 2007, he 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, which established the reporter's privilege for online journalists.

Sandra Ordonez is the former communications manager for Wikipedia, and external communications lead for Joomla.

Jennifer Ortiz is a pharmacist and web developer with a special interest in toxicology. She graduated from Rensselaer Polytechnic Institute with a B.S. in electronic media arts and communication and a minor in computer science. She earned her Pharm.D. at Creighton University in 2012.

Howard Payne is an elevator consultant from New York specializing in code compliance and accident investigations. He has logged over 9,000 hours examining car tops, motor rooms, and hoistways in cases ranging from minor injuries to highly publicized fatalities, and has contributed to forensic investigations that have been recognized by local, state, and federal courts. Howard has appeared on national broadcast television making elevators do things they never should. When he's not riding up and down high-rise hoistways, he moonlights as a drum and bass DJ and semiprofessional gambler. His favorite direction is up and his favorite elevator feature is riot mode.

Nadya Peek is a PhD student at the MIT Center for Bits and Atoms, and works on digital fabrication and technology for humans. Their projects include distributed control systems, foldable multipurpose fabrication tools, and reconfigurable machines for making.

Jeremy Pesner specializes in issues of technology policy related to user-oriented innovation and collaboration. He maintains involvement with the Wikimedia Foundation, the Journal of Science Policy and Governance, FedScoop, and the STGlobal conference. He is a fellow of the StartingBloc Institute for Social Innovation and Internet Society Next Generation Leaders Programme).

Dan "AltF4" Petro is a senior security analyst at Bishop Fox, a security consulting firm providing IT security services to the Fortune 500, global financial institutions, and high-tech startups. In this role, he focuses on application penetration testing and secure development. He holds a Bachelor of Science with a major in computer science as well as a Master's degree in computer science from Arizona State University.

Tiffany Strauchs Rad is an attorney, professor, and senior computer security analyst who has spoken on reverse engineering and the Right To Repair Act. She is co-author of the book *Security in 2020* and her security, legal, and policy research has been featured in publications and media such as *60 Minutes*, *Washington Times*, NPR, *MIT Technology Review*, *PC World*, *Popular Mechanics*, Ars Technica, *Der Spiegel*, *2600: The Hacker Quarterly*, CNN, *Wired Magazine*, Reuters, *Huffington Post*, and others.

Jesselyn Radack is a legal advisor to Edward Snowden and has represented many of the whistleblowers charged under the Espionage Act. She is the director of National Security and Human Rights at the Government Accountability Project (GAP), the nation's leading whistleblower organization. She has been at the forefront of the government's unprecedented "war on whistleblowers," which has also implicated journalists and hacktivists. Among her clients, she represents seven national security and intelligence community employees who have been investigated, charged, or prosecuted under the Espionage Act for allegedly mishandling classified information, including Edward Snowden, Thomas Drake, and William Binney. Previously, she served on the DC Bar Legal Ethics Committee and worked at the Justice Department for seven years, first as a trial attorney and later as a legal ethics advisor. She is author of *TRAITOR: The Whistleblower and the "American Taliban."* Her writing has appeared in the *New York Times*, *Wall Street Journal*, *Los Angeles Times*, *Washington Post*, *Guardian*, *The Nation*, *Salon*, and numerous academic law reviews.

Steve Rambam is the founder and CEO of Pallorium, Inc. (http://www.pallorium.com), a licensed investigative agency with offices and affiliates worldwide. He has coordinated investigations in more than 50 countries and in nearly every U.S. state and Canadian province. Steve has conducted or coordinated numerous foreign insurance-related investigations, including hundreds of homicide and "death claim" investigations, and a significant number of these cases have resulted in confessions, arrests, and prosecutions. He is perhaps best publicly known for his pro bono activities, which have included the 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. Steve is currently co-authoring a non-fiction book, *Stealing Your Own Identity*, and he is the subject of a second non-fiction book, *Rambam, P.I.*

Michael Ravnitzky is an attorney, engineer, and former journalist who has co-founded several First Amendment-related websites, including GovernmentAttic.org.

Ray is a hacker and lockpicker from Germany. Besides having a master's degree in computer science and interests in Unix/Linux security, he's been collecting and picking all kinds of locks for over a decade and has given presentations in the Netherlands, Germany, and the United States on related topics. You may have seen his previous talks about locks and handcuffs at past HOPEs. Ray is also a founding member of his local CCC organization and leads the Munich chapter of Sportsfreunde der Sperrtechnik (SSDeV), Germany's largest LockSport group.

Garrett Robinson is the lead developer on SecureDrop. His interest in empowering whistleblowers through technology began when he was involved with environmental activism in Appalachia, and lead to the creation of a whistleblower submission site named Honest Appalachia. He currently works full time as a security and privacy engineer for Mozilla, and previously worked for the EFF.

Marc Rogers aka cyberjunky is an English hacker, director of SecOps for Defcon, and a past speaker/staff member for HOPE. These days, Marc works as principal security Rresearcher for Lookout.

Ed Ryan is a New York patent attorney with a background in physics who deals with technologies including digital broadcast, semiconductor design, hula hoops, and (omg) software patents.

Eleanor Saitta is a hacker, designer, artist, writer, and barbarian. She makes a living and a vocation of understanding how complex, transdisciplinary systems operate and redesigning them to work, or at least fail, better. Among other things, she is a cofounder of the Trike project (http://octotrike.org), technical director at the International Modern Media Institute (http://immi.is), a member of the advisory boards at the Freedom of the Press Foundation (https://pressfreedomfoundation.org) and Geeks Without Bounds (http://gwob.org), a contributor to the Briar project (http://briar.sf.net), and a freelance security architecture and strategy consultant. She is nomadic and lives mostly in airports and occasionally in New York, London, and Stockholm. She can be found at http://dymaxion.org.

Jonathan Schiefer has been writing scripts since 2002. In 2010, he began making commercials and short films. He is now an independent filmmaker who believes the industry needs to change. He's doing his best to make that change a reality. *Algorithm* is his second feature-length movie.

Douwe Schmidt is a community manager and privacy advocate. As part of his work at Dutch hosting provider Greenhost, he organizes the monthly meetup TA3M and founded the critical community Noisy Square - a coalition of many organizations and individuals questioning the dynamics of the net on a fundamental technical and political level. Currently, he is a volunteer for digital rights organization Bits of Freedom, for which he collaborates with many Dutch organizations to make a nationwide crypto party called Privacy Cafe. This initiative recently spread out to other countries like Belgium and France. He is also the author of a research blog on his digital alter-ego in which he investigates the data hunger of governments and of companies.

Jason Scott is a troublemaker. He makes up for being a troublemaker by being a really loud troublemaker. In cases where this is not warranted, he becomes a screaming ranting chair-throwing troublemaker. He runs textfiles.com, has made several documentaries, and is lightly amusing.

Geoff Shively is a former Telecomix agent, company starter, and idea tinkerer.

Michael Sikorski is a well-known expert in malware analysis and co-author of the No Starch Press book *Practical Malware Analysis*. He is a technical director at Mandiant, where he runs the malware analysis team. His previous employers include the National Security Agency and MIT Lincoln Laboratory. Mike frequently teaches reverse engineering to global audiences.

Per Sjoborg runs a blog and a podcast focusing on self-reconfiguring modular robotics (SRCMR) at www.flexibilityenvelope.com. He also does general robotics interviews for www.robotspodcast.com. Per has been doing this since 2005 and attends many robotics conferences to learn more. He trained as a mechanical engineer with a focus on FEM calculation. He spent ten years as a programmer and ten years doing hands-on property management, and right now is in the process of starting a number of robotics related businesses to get some skin in the game.

Kurt Snieckus is an electrical engineer and part of NYC Meshnet. He wants the mesh to provide a cheap, safe, and reliable community network for distributed services as well as competition to traditional ISPs.

Edward Snowden will forever be known as someone who changed history, not only in this country, but throughout the world. His revelations of the massive NSA surveillance programs confirmed the suspicions of many and shocked those who haven't been paying attention. Throughout it all, he has remained strong and true to his convictions, while forced to remain in Russia to avoid the severe punishment virtually guaranteed by the United States government. Had these truths not been revealed, most people wouldn't have a clue of the extent of privacy violations they face every day at the hands of intelligence agencies. Even conferences like HOPE wouldn't be devoting nearly as much time to the subject without what has been learned over the past year. We are humbled to have him in our program, and hope the day will come when he's not confined to a video link and able to be as free as he is helping all of us to be.

Christopher Soghoian is a privacy researcher and activist, working at the intersection of technology, law, and policy. He is the principal technologist with the Speech, Privacy, and Technology Project at the American Civil Liberties Union. He completed his Ph.D. in 2012, which focused on the role that third party service providers play in facilitating law enforcement surveillance of their customers.

David Solomonoff is president of the Internet Society - New York chapter, and is the library systems manager for the State University of New York (SUNY) Downstate Medical Center. He serves on the Technology Issues and the Globalization and Corporatization committees of United University Professions (UUP), the labor union representing SUNY faculty and staff. He recently became a member of ICANN's working group for new global top level domains (GTLDs).

Robert Steele, former spy, honorary hacker, and #1 Amazon reviewer for nonfiction, has also set the world record for Q&A at eight hours and one minute, going from midnight Saturday to 0801 Sunday at The Next HOPE (2010). In 2012, he was accepted by the Reform Party as a candidate for the presidency. The son of an oil engineer, he has lived all over the world, been a Marine Corps infantry officer, a CIA clandestine case officer, a founder of the Marine Corps Intelligence Center, and a CEO of both a for-profit (OSS.Net, closed in 2010) and a nonprofit (Earth Intelligence Network).

Lisha Sterling is the developer coordinator at Geeks Without Bounds, an accelerator that supports open source humanitarian projects through hackathons and mentorship. She has been a software developer for over 20 years and was the TA who helped develop and teach one of the first college level courses in political science about the Internet and its use in activism at College of Alameda in 1995.

Becky Stern is the director of wearable electronics at Adafruit. Each week, she publishes a new do-it-yourself craft+tech project tutorial and video and also hosts the YouTube Live show "Wearable Electronics with Becky Stern" (adafruit.com/beckystern). She's been combining textiles with electronics since

2005. She is a member of the Brooklyn art combine Madagascar Institute and the Internet-based group Free Art & Technology (FAT).

Kristen Stubbs is a queer/pansexual roboticist who's more interested in people than in technology. Kristen earned her Ph.D. in robotics from Carnegie Mellon University in 2008. She runs the sex-positive startup Passionate Produce (passionateproduce.com), blogs about her own experiences with sexuality and pleasure (toymakerproject.com), and organizes a sex/kink-positive maker meetup group (teasecraft.com). Kristen's light-up dildo prototype "The Hammer" was awarded a Golden Kleene at Arse Elektronika 2012 and has been named the #1 Geekiest Sex Toy by Cracked.com.

Todd Sundsted is a professional programmer, a writer, and an entrepreneur who has been building software for over 20 years. He currently lives in New York City, has worked for companies ranging in size from Bloomberg LP (big) to SumAll (small), and has worked on everything from programming languages, to mobile applications, to infrastructure, storage, and scaling.

tante lives in the Internet and (under the alias Jürgen Geuter) in the German meatspace where he works at a small university. He's been writing about the future of us as networked beings and the way technology changes the (social) world on his blog (tante.cc) and other publications. Apart from thinking about the digital sphere, he likes monkeys.

TProphet, also known as The Telecom Informer, is a regular columnist for *2600: The Hacker Quarterly*. As a young phreak, he began exploring the world through the phone system. He has now visited all seven continents and writes the popular *Seat31B* travel blog.

Peter Valdez is a programmer with the goal of using technology for good purposes. He manages and runs meetings for NYC Meshnet, a group dedicated to establishing New York City's own mesh network.

Jurre van Bergen (Dr. Whax) is a software developer at Greenhost. He contributed to the technical realization of Publeaks and Wildleaks. He is one of the founders of Technologia Incognita, contributes to several software projects, is treasurer of Hart voor Internetvrijheid, and was one of the organizers of NoisySquare at OHM2013.

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. Sacha has a background in science and technology studies, artificial intelligence, and law. From this background, he can relate to the technical aspects as well as to the social and political aspects of technological change.

James Vasile directs the Open Internet Tools Project, which supports development of free software anti-censorship and anti-surveillance tools. He is a partner at Open Tech Strategies, which advises organizations and businesses as they navigate the open-source world. He is also a senior fellow at the Software Freedom Law Center, where he acts as a strategic advisor on a range of free software efforts. James has helped boot up a number of free software organizations, including the FreedomBox Foundation, Open Source Matters, and the Software Freedom Conservancy.

Stephen Watt is the lead developer of Dark Mail's reference implementation. He is best known for his 2009 conviction for the TJ Maxx data breach. For merely writing a piece of software that was used by others to sniff customer data, he was given a two year federal prison sentence and ordered to pay $171.5 million in restitution. Because he refused to cooperate at all with the federal investigation into himself and his friends, he emerged from prison with his pride intact. Since his 2011 release, Watt has spoken at several security conferences about his extraordinary legal experience. By joining the Dark Mail initiative, he hopes to continue a lifelong pattern of developing massively disruptive software with complete indifference to getting rich from it.

Vivien Lesnik Weisman is the director of the new film *The Hacker Wars*, a feature length documentary about the targeting of hactivists by the U.S. government. The film is in post-production. Her last film, *Man of Two Havanas*, was met with critical acclaim and has gone on to win many prestigious awards throughout the world. She is also a regular contributor to *The Huffington Post*.

Jos Weyers decided to do some training after ending second in the ongoing toool.nl competition four times in a row. Four hundred key blanks later, he slashed the then world record time of four minutes and 23 seconds to impression an Abus C83 (he did it in 87 seconds). He's the Dutch champion (two times in a row), and German Meister (that's champion in German, also twice), and current world record holder in this particular lock opening technique. Jos is the vice president of toool.nl. Most people know him as the Dutch kilt guy.

Beau Woods is an independent security consultant and an early participant in the I Am The Cavalry movement.

Andrew Yoder has been listening to, writing about, and speaking about pirate radio stations, particularly on shortwave, for more than 30 years. He has written *Pirate Radio Stations* (1990, TAB Books), *Pirate Radio* (1996, HighText), *Pirate Radio Operations* (1995, with Earl T. Gray, Loompanics), *Pirate Radio Stations* (2000, McGraw-Hill), and *The Pirate Radio Annual* (2010-2014, Hobby Broadcasting). His blog is at: http://hobbybroadcasting.blogspot.com.

Sarah Zatko is a partner at L0pht Holdings LLC, the spin off from the L0pht that created the award winning password cracking tool L0phtCrack. She holds a degree in mathematics from MIT, and a Master's in computer science from Boston University. After working with various three letter agencies, she wanted to do something unequivocally "good" and has been visiting high schools and elementary schools representing "hacker" on career day. She's trying to convince her local library to let her teach a lockpicking workshop.

Jonathan Zdziarski is considered to be among the foremost experts in iOS related digital forensics and security. As an iOS security expert in the field (sometimes known as the hacker NerveGas), his research into the iPhone has pioneered many modern forensic methodologies used today, and has been validated by the United States' National Institute of Justice. Jonathan has extensive experience as a forensic scientist and security researcher specializing in reverse engineering, research and development, and penetration testing, and has performed a number of red-team penetration tests for financial and government sector clients. He frequently consults with law enforcement and military on high profile cases and assists federal, state, and local agencies in their forensic investigations, and has trained many federal, state and local agencies internationally. He has written several books related to the iPhone including *iPhone Forensics*, *iPhone SDK Application Development*, *iPhone Open Application Development*, and his latest, *Hacking and Securing iOS Applications*.

Yan Zhu is a staff technologist at EFF, specializing in projects to protect Internet users' privacy and maximize the use of encryption on the web. She is the lead maintainer of EFF's browser security extension, HTTPS Everywhere.

PROJECTS

2600 Store

HOPE would never exist without its founder and sponsor, *2600 Magazine*. And because HOPE doesn't make a profit, it couldn't happen without sales of *2600* merchandise. So show your support for this amazing project - and for the longest-running (30 years!) English-speaking hacker magazine on the planet - by buying some issues, books, DVDs, calendars, shirts, hoodies, caps, mugs, stickers, and more. Bring home some gifts from HOPE X to let your friends know you were here. And thanks for your support!

Friday through Sunday - 18th Floor

Amateur Radio Station W2H

Amateur radio operators, or "hams," have been developing and hacking wireless electronic communications for over a century. Their work helped give birth to the hobby electronics and hacker movements, cellphones, Wi-Fi, and much more. The FCC has granted HOPE X a special-event amateur radio station license to demonstrate the radio arts. Check out station W2H on the 18th floor and see free global voice/data communication - with *no infrastructure!* It's fun and a great global community to be part of - and it *always* works - even when your cell phone and Internet infrastructure fails! Throughout the weekend, radio station W2H will attempt to establish two-way digital radio contact with the International Space Station as it passes over HOPE X. Stop by and see how easy it is to establish free global communications without any infrastructure!

Friday through Sunday - 18th Floor

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 acclaim by the American hacker community. Since then, we've supplied hackerspaces and rock stars with pallets of this stuff. Get yourself a cold half-liter bottle of Club-Mate or a whole case, and stay up and energized throughout HOPE X.

Friday through Sunday - Mezzanine

Fourth Track - Free Speech at HOPE X

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 YOU room 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. Scheduling is first-come, and details on how to sign up will be announced at the start of HOPE and posted by the YOU Room on the 18th floor.

Friday through Sunday - YOU

General Demo Area

Throughout HOPE X there will be a variety of informal free-format demos of all kinds of interesting projects you might want to get involved in. If you have something you've been working on that you want to show off, this is the place. It's like a "show and tell" for the hacker community.

Friday through Sunday - Mezzanine

Hacker Village Areas

It's like an outdoor hacker camp village, but inside the HOtel PEnnsylvania. The Hacker Village Areas (A and B) have 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 HOPE X. Stop by the Village Areas 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.
Friday through Sunday - Mezzanine

InfoDesk

Got a question about anything at HOPE X? 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 in the "Village Area"

Mitch Altman and friends will bring kits to make cool, practical, intriguing, open source, hackable electronic devices that you can build and bring home. You can quickly and easily learn all the electronic construction skills you need to build a cool project. If you have something to fix, bring it by. If you would like help, or want to have your questions answered, this is the place. It's fun to make things with other people in this friendly community of hackers and makers. Come join us. Everyone is welcome!
Friday through Sunday - 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 will be on hand to demonstrate - and plenty of locks, picks, shims, and other devices will be available.
Friday through Sunday - Mezzanine

Movies at HOPE X

HOPE X will host several first-rate movies on Friday and Saturday nights, and a TV network premiere will be screened at noon Saturday. These presentations are all highly relevant to the hacker community and were carefully chosen and solicited for your viewing enjoyment. Film directors will introduce their work and do Q&A afterwards. In some cases, free popcorn and movie gift giveaways can be enjoyed. Check your schedule for more details.
Friday, Saturday (check your schedule)
Location: 18th Floor

Press Room

HOPE X is pleased to host the largest number of world-class and indy 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 HOPE X like no other HOPE before. Journalists can take advantage of a secluded and quiet(er) space adjoining the facilities of Radio Statler to conduct one-on-one interviews with the hundreds of HOPE X speakers, panelists, workshop presenters, project managers, organizers, volunteers, and others to give their media outlet's readers, listeners, and viewers the real story at HOPE X. Journalists - get your scoops here!
Friday through Sunday - Mezzanine

Retrocomputing - Vintage Computer Exhibit

MARCH (Mid-Atlantic Retro Computing Hobbyists) will present a truly historic selection of working vintage Apple computers for you to try out. This includes an exquisitely-detailed Apple 1 replica, an Apple][, several Apple][clones, Apple ///, Lisa, Macintosh, and Mac Portable - plus some surprises! Come get your retro-geek on with these vintage microcomputers, and learn tech trivia from the encyclopedic experts of MARCH.
Saturday, Sunday - Mezzanine

Security/First Aid

Lose your mobile phone or wallet? It's way more likely to be turned in at the HOPE X Security desk than outside on the street! There are *no* security goons at HOPE X. 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 - 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 makes this unique transportation machine worth trying out. The HOPE X 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, tools, tee shirts, lockpick set and tools, electronic kits, 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

HOPE CONCERTS

Join us for TWO NIGHTS of some of the East Coast's finest music made with circuits, game consoles, odd objects and radio. GUS once again presides over the blippery, whipping each non-moving booty of the hacker populace into an electric frenzy Tesla would have been proud of. Why shake it? Rule 34. (Remember, you're somebody's fetish. No exceptions.)

Friday

Opening at 11:00pm with AMIGOS PODEROSOS, the new techno project by José Olivares of Balún fame! At 11:30pm, join CORSET LORE for revelations of a Gameboy unbound! The witching hour brings ZEN ALBATROSS, set to exploit waveform synthesis on antiquated computer systems! And rounding out the first night of HOPE X concerts, RADIO WONDERLAND will turn mass media into recombinant techno with a boombox, steering wheel, and shoes!

Visuals from NO CARRIER, CHIKA, FUTURESTACK, and VBLANK (in order of appearance).

Saturday

At 11:00pm, the bodhisattva of chip and non-chip styles himself, mista MINUSBABY, followed by the giddy Sega-hued jazz of SYLCMYK! Tonight's witching hour brings the inimitable lo-fi, hi-class sounds of BUBBLYFISH! And rounding out concert night #2 for HOPE X is GRABTHAAR, a solo set from Justin Emmerson of Burnkit 2600 renown!

Once again, we will be joined by the previous night's visualists for a fine evening of low-res smashy-smashy. FUTURESTACK, CHIKA, NO CARRIER, and VBLANK (in order of appearance).

HOPE ARTSPACE

The artists assembled for HOPE X represent a confluence of disparate backgrounds, technologies, and techniques unified in challenging the surveillance culture that has come to dominate the early 21st century.

The Book Machine
Kevin Carter
The Book Machine is a small wireless router that broadcasts art (including books, music, and images) to any device that connects to it.

Just For Your Security
ST
Just For Your Security examines the global surveillance and espionage scandals through an installation of five works exploring the intrusion of intelligence agencies into our private lives.

Logo Removal Service
Miriam Dym
Dym transforms the mass-produced into the particular through the complete removal of unwanted logos, brands, marks, etc., replacing them with unprecedented and unrepeatable shapes in surprising colors.

PER SPECULUM IN ÆNIGMATE
Max Clarke
A series of prints about privacy that also functions as a secure messaging system combining PGP encryption, QR codes, and anaglyph 3D nudes.

RADIO WONDERLAND
Joshua Fried
Fried turns live mass media from a boombox

blaring FM radio into recombinant techno (in real time) via computer processing, controlled by a Buick steering wheel and old shoes hit with sticks.

Sketch3D
Kelly Egan
An application that allows users to draw in 3D space. Users utilize a combination of wireless and gesture-based controls to create, manipulate, and export complex 3D drawings.

Surveillance Collage
Andrew Lloyd Goodman
A generative video collage that combines fragments of still and moving images with live video footage to create a dynamic and dystopic mirror of current events.

Upon Graphene
Shane Hope
Painterly 3D-printing depictions of non-nonobjective molecularity.

X.pose
Xuedi Chen
X.pose is a wearable data-driven sculpture that changes opacity to expose a person's skin as a real-time reflection of the data the wearer is revealing.

WORKSHOPS

CONTINUOUS

Amateur Radio at HOPE X - Radio Station W2H
18th floor hallway

Hacking the Commodore 64
Mezzanine Demo Area

Learn to Solder / Variety of Cool Kits!
Mezzanine Village Zone A

Noisy Square & Chill Space
Mezzanine Village Zone B

Transparency Toolkit
Mezzanine Demo Area

FRIDAY

Getting up and Running with Encrypted Communications
1230-1500 6th floor small room

FOIA 101 - Basic FOIA Workshop
1330-1430 6th floor large room

FOIA Advanced Strategies and Tactics
1500-1600 6th floor large room

Screening LGBT Film in China: from street to family
1530-1630 6th floor small room

Building and using an ITC "Spirit" Image Capture System
1600-1900 Mezzanine Village Zone B

SATURDAY

Extensively Adaptable Sploits and Tools for Encroaching on Router Security
1000-1330 6th floor small room

Birds Of A Feather Meetup -- Educators and Technology
1100-1200 6th floor large room

Arduino For Total Newbies
1300-1630 Mezzanine Village Zone A

Pop Up Repair
1300-1600 Mezzanine Village Zone B

How to Build and Run Your Own Cellular Network
1300-1700 6th floor large room

Navigating the Dark Net
1430-1600 6th floor small room

Designing Custom Circuit Boards with Eagle CAD
1630-1830 6th floor small room

Electric Waste Orchestra: Build Musical Instruments from E-Waste
1830-2230 Mezzanine Village Zone A

Birds Of A Feather Meetup -- Security Usability
2030-2130 6th floor small room

SUNDAY WORKSHOPS

Amateur Radio FCC Exams
1000-1300 6th floor small room

Mindfulness Meditation for the Digital Age Activist: Discovering Sanity in a Maddening World
1100-1300 6th floor large room

Using a Data Glove as Musical Instrument
1300-1700 Mezzanine Village Zone B

DIY LED lighting with the BlinkyTape
1330-1530 Mezzanine Village Zone A

Maker Party with Mozilla To Hack the Web
1400-1600 6th floor small room

Noisy Square

Throughout HOPE-X, the Noisy Square will be a self-organized community for critical thinking, discussions, theorizing and politics. Come and question the fundamentals of all of the systems we rely on. There will be ongoing workshops that you can take - or give: politics, society, UX . . .

Noisy Square will also host a Chill Space throughout the duration of HOPE-X, with music and discussions and perhaps some nice tea. Come chill and relax.

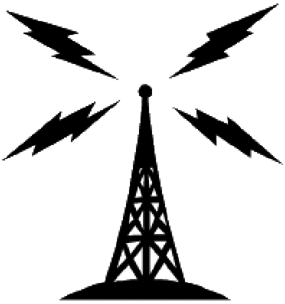
RADIO STATLER

Do you have something to say? Do you want to help bring HOPE to the world? Stop by Radio Statler on the 2nd floor and join us as we broadcast original material and expanded conference content to the wide reaches of the Internet. Radio Statler is HOPE's 24-hour live streaming audio station, named after the New York Statler Hotel, which is what the Hotel Pennsylvania used to be called a long time ago.

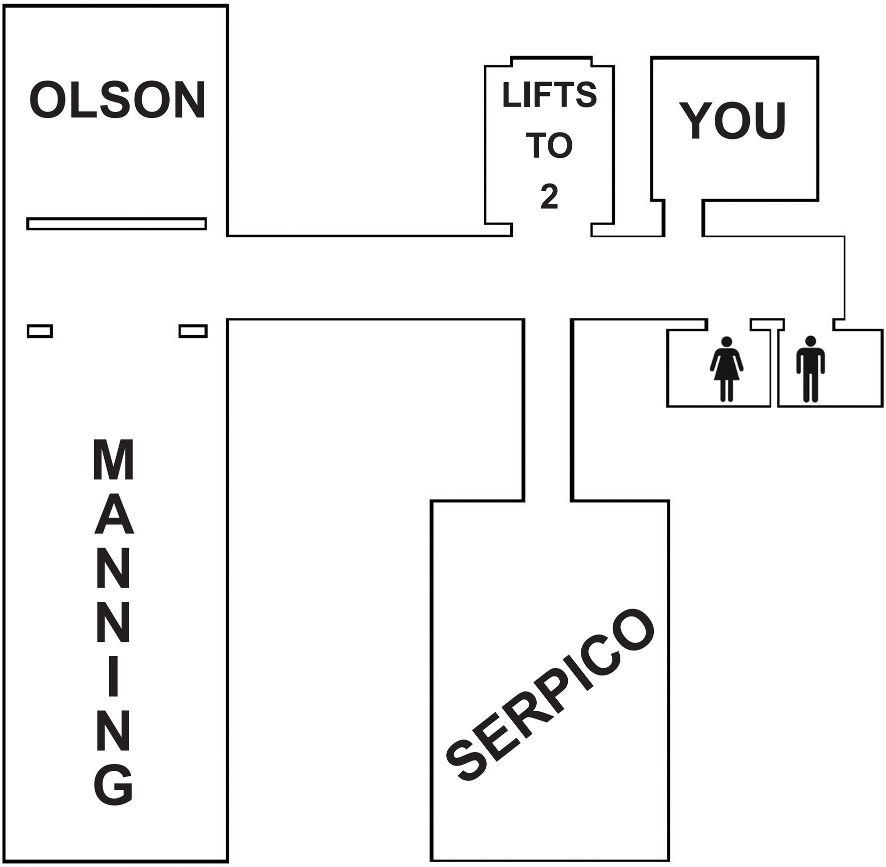
Radio Statler features original HOPE content such as interviews of HOPE speakers, workshop presenters, artists, musicians, exhibitors, staff, and attendees. Radio Statler also broadcasts a live HOPE edition of *Off The Hook*, select moments and outtakes from previous conferences, and the live chiptunes concerts on the first floor of the conference. Roving reports will also provide timely updates of the excitement on the conference floor.

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. You can find us behind the security area, across from the art exhibits.

Know someone who can't make the conference? Tell them to listen to the Radio Statler audio stream at http://radio.hope.net/ - The Voice Of HOPE!



EIGHTEENTH FLOOR



Flip to the inside front cover
for second floor information

THANK YOU

We'd like to thank all of our attendees, volunteers, vendors, and the following generous sponsors for helping make HOPE X possible

cornfield electronics

MANDRILL

The Daily Dot

net@ccess CORPORATION

HE HURRICANE ELECTRIC INTERNET SERVICES