From: Webb, M., Coding Democracy (MIT Press, 2020).

1

THE HACKER ETHIC

Germany's Chaos Computer Club and the Genealogy of the Hacker Ethos

IN BERLIN

Berlin still has many bombed-out lots. If you peer in behind the mesh fences, you see deep craters that sink precipitously under a cover of decades-old trees. These holes seem to perforate the psyche as well as the landscape of the city. Some are the size of city blocks, some the size of small neighborhoods, and some are just green spaces where large tracts of city and inhabitants have ceased to exist as geographic facts.

In photos of the postwar period, the Reichstag building is often visible, with Germans picking their way around its large, defeated hulk on foot and on bicycles, the road a track of mud. The seat of German democratic government in Berlin, the Reichstag was notoriously set on fire in 1933, then scorned by Adolf Hitler (he never used it), and badly bombed by Allied planes. The Germans left it unreconstructed until well into peacetime, living with its wreckage until it was finally patched up for use in the 1960s and fully renovated in the 1990s. The dome of the renovated Reichstag echoes the burned-out, twisted dome of the old building and is encased in glass—a symbol, perhaps, of both contrition and transparency.[1]

Walking around the bomb sites, the broken wall, and the sooty, uncared-for imperial buildings of Berlin, a visitor might wonder whether these two values, contrition and transparency, can exorcise the dark

history of the place, which in the twentieth century went through multiple paroxysms—two wars of aggression, wild excess and inflation, mass deportations and murder, totalitarian surveillance, and a grim physical division. Despite a new German narrative of economic recovery and openness, Berliners still live amid the ruins of their elites' many bad decisions. They tend to be people with few illusions.

It's no coincidence that a strong hacker culture has taken root here and flourished.

GETTING TO THE CHAOS COMMUNICATION CAMP

The Chaos Communication Camp happens every four years. The trouble is, every four years its attendance seems to double. In 2015, its organizers are struggling to accommodate 4,500 camping hackers. The website of the Chaos Computer Club (CCC), the group that organizes the camp, still says,

> ~~The Chaos Communication Camp is an international, five-day open-air event for hackers and associated life-forms. It provides a relaxed atmosphere for free exchange of technical, social, and political ideas. The Camp has everything you need: power, internet, food and fun. Bring your tent and participate!~~

But it also says:

> ~~Verpeiler friends' request? If you don't get your ticket on Friday, you will have one very last, very tiny chance. Go to the ticket system and convince us that you are one of our dearest verpeiler friends. There won't be many of those tickets available. Also you need to be very patient waiting for a reply~~ … **We are sold out!**

I've come to Berlin on the fly. I've failed to obtain tickets to the camp by any means, but through an American lawyer I know, who knows a prominent German lawyer, who knows one of the main organizers of the camp, I've managed to score a ride this late afternoon of the first day of the event, and that's a relief.

I'm here to do research, to talk to people in the hacking world, and I'm keenly aware I'm starting this book project with only a moderate amount of knowledge about what hacking and code are. I wrote a book on mass surveillance, *Illusions of Security: Global Surveillance and Democracy in the*

Post-9/11 World (2007), which came out six years before Edward Snowden made his disclosures of highly classified National Security Agency (NSA) materials. The book predicted much of what Snowden's leaks revealed about the scope of government and private-sector surveillance and its dangers for democracy. At the time, I had hoped constitutions in Western democracies would be strong enough to roll back these abuses once they were uncovered. But lately, I've become convinced this is not going to happen. When you take stock of the pervasive illegality states and corporations are engaged in with their uses of digital tech, it is manifest the law is collapsing.

In this era of rising instability, a digital revolution is unleashing forces that are not well understood by citizens and their elected officials. As the mass surveillance, concentrations of power, and authoritarianism enabled by digital tech grow around the globe, millions have begun to worry where this new century is taking us. Can societies hold onto and, indeed, "build out" democracy into cyberspace in the digital age?

Code, more than law, will soon determine what kind of societies we live in and whether they end up resembling democracies at all. Yet code is incomprehensible to most people, myself included. Computer users, for the most part, are at the mercy of the code makers.

Who controls code? This is the urgent civics question that's spurred the journey I am about to make through the world of hackers and hacking, a journey that, before I am done, will take me to Berlin and the Chaos Communication Camp and also to Barcelona, Rome, Boston, Cambridge, San Francisco, Vancouver, and the Gulf Islands in the Salish Sea. In many respects, it is an everyperson's journey, and I am that everyperson—not a hacker, technologist, or academic who studies hackers but rather a labor and constitutional lawyer, a Canadian, a trade unionist, a parent trying to raise children and hold down a regular job, and one of millions of ordinary citizens in Western countries concerned about our democracies in this new century. Although this journey might prove challenging for someone like myself without tech expertise, I'm convinced it's a journey every citizen must make to understand what is happening to democracy in the twenty-first century.

A struggle is taking place right now as corporations, states, criminal elements, and parts of civil society vie to build the coded environment around us. Hackers are savants in this world. But their identity is protean.

Sought after for their talents, almost folkloric in status, they've been recruited and reviled, celebrated and thrown into prison.

I'm familiar with the stereotype of hackers as dangerous, nihilistic elements in society who are capable of bringing down critical infrastructure and sowing strife between nations. These are real threats, not to be minimized. Yet I know enough to believe hackers might also be vital disruptors in the emerging digital environment, with its dystopic, antidemocratic tendencies. There is an astounding array of hacker experiments underway right now that could fundamentally change the current political economy.

More than this, I see hacking becoming a practice, an ethos, and a metaphor for a growing social movement in which ordinary citizens are taking things into their own hands when reform seems out of sight. At a time when people's faith in elites to govern has never been lower, I see hacking inspiring a new wave of activism, a new way of thinking and acting, as citizens fight to take back their democracies.

As I wait on the sidewalk for the ride that will take me to the hacker camp this summer day in Berlin, I feel strongly that I'm writing this book for tech insiders as well, for them to reflect on where hacking has come from and where it might be going, and on the processes by which the knowledge they possess might urgently be transferred to the mind of the ordinary citizen. My intent on this journey is not to valorize the hacker, Silicon Valley visionary, counterculture guys' club, Harvard professor, or MIT hotshot—necessary as it is to situate their remarkable stories and credit their innovations in the genealogy of hacking. My intent is to celebrate the hacking ethos, the collective intelligence of people, and the spirit in all of us to resist domination and unfairness. The stories at the heart of this book will be about citizen hackers who are inventing new forms of distributed democracy. Its central question will be how we ordinary citizens and tech insiders go forward together to accomplish the hard work of democracy in the digital age. It won't be easy, but we've got to try.

My ride today is with Andy Müller-Maguhn. People have told me that Andy is the *ur* German hacker—meaning the earliest, the original, the prototypical German hacker. He pulls up behind the wheel of a black diplomatic series Mercedes sedan, complete with automated curtains on the

windows. He doesn't stop right at the curb but askew to it, like someone on the move. He's wearing a vinyl version of a hipster's pork pie hat. The man beside him in the passenger seat introduces himself as Peter, from Sweden. I climb in and am immediately enveloped by the Mercedes's sound system, pulsing with '90s techno music.

The Chaos Computer Club, which Andy has been associated with since its early days, was founded in 1982. It has been involved in all the major digital tech debates of the last four decades, and its role in the unfolding story of hacking in the early part of the twenty-first century is central. The club began, so the story goes, around a table that once belonged to the notorious counterculture group Kommune 1. A communal group in West Germany in the 1960s, Kommune 1 practiced performance politics, free sex, and experimental drug use, attracting a glamorous entourage that included the late Jimi Hendrix. The table belonged to the German Green Party at one point, and by the time it entered the self-conscious mythology of the hacker group, it was in the rooms of the progressive newspaper *Die Tageszeitung*. The Chaos Computer Club's founder, Herwart Holland-Moritz, also known as Wau Holland, wrote occasionally for the paper and was an early digital rights pioneer in Germany.

The CCC's first annual Congress was held, aptly, in 1984. A few hundred people were present. Today, the Chaos Computer Club is Europe's largest association of hackers, and close to ten thousand people attended its congress in 2014.[2] Like Nelson Mandela's African National Congress, its reputation has morphed over time from suspected criminality to fashionable respectability.

Andy, Peter from Sweden, and others have been working for the past year to organize the camp, but Andy doesn't like camping and will not be staying over. Tough-minded and politically sophisticated, Andy has been in the thick of things for a long time. Just how much in the thick, I sense, he might not want to say, and it might be bad form to ask.

FIRST-WAVE HACKERS: HACKING CULTURE IN THE US FROM THE LATE 1950S, INCLUDING THE HANDS-ON IMPERATIVE AND OTHER PRINCIPLES OF A HACKER ETHOS

Hacker culture's earliest origins were not in Europe but in the United States, where hacker culture began in the 1950s at academic institutions

that had early, mainframe computers. That might seem a long-ago place to start a story about contemporary hacking, but hacking is a story about a genealogy of ideas as much as anything—ideas as they are lived, distilled, built on, repurposed, and disseminated by hackers, just as code is. In this chapter, I give a brief history of the beginnings of hacking and the hacking ethos in the United States and Europe from the 1950s through the 1990s and attempt to leave the reader with a first impression of the Chaos Communication Camp, too.

The story begins at the Massachusetts Institute of Technology (MIT). *Wired* magazine journalist Steven Levy wrote a seminal book in the mid-1980s on the history of hacking called *Hackers: Heroes of the Computer Revolution*.[3] It is a dense yet entertaining book that everyone who hacks or writes about hacking references yet seldom revisits and unpacks. Levy's descriptions of the early MIT hackers and the ethic he ascribed to them are worth recounting in detail because Levy's distillation of that ethic has been picked up, *verbatim*, by progressive political hacker scenes in the twenty-first century, including the burgeoning scene coalescing around the Chaos Computer Club. While Levy's distillation may not be universally subscribed to, it's been very influential in contemporary hacking. Insiders who know the early history of American hacking, which Levy recorded, may want to skip forward to my exposition of early hacking in Europe or to my detailed account later in this chapter of the Chaos Computer Club's history. But for ordinary computer users trying to understand contemporary hacking, the next few pages will be foundational.

Levy described how a hacking culture first grew at MIT among engineering and physics students coalescing around a club that built an elaborate model train set in MIT's Building 20. As the electronic routers the club designed became ever more complicated and the group scrounged around the halls of MIT at night looking for parts, they discovered early "keypunch" machines in the basement of Building 26. These machines produced the "punch cards" that were the programming medium for an early IBM 704 computer housed on the building's first floor. Thirty tons and nine feet tall, the IBM computer was off limits to students, but they managed to sneak into the basement room at night and play with the keypunch machines, inventing new "programming" solutions for their railway system. In 1959, when MIT offered the first computer

programming course for freshmen, these enthusiasts signed up. What they really wanted was to get their hands on the IBM computer itself. But there was an elaborate bureaucratic system of rules around these bigger machines to keep tinkering-obsessed students from tampering with them.

The most proficient tinkerers in the model railroad club called themselves, self-deprecatingly, "hackers." They might call a clever patch they had made "a mere hack" or say that they were "hacking away" at the railway routing system—*hacking* in the dictionary sense meaning "to cut or sever with repeated irregular or unskillful blows; to cut or shape by, or as if by, crude or ruthless strokes; … to play inexpert golf." Early radio geeks had called themselves "hackers," and there was a long tradition at MIT (which persists today) of students engineering elaborate, playful pranks, called "hacks" (such as covering the great dome of Building 10 with tin foil or building a police patrol car on the dome, replete with flashing lights and a box of donuts).

When one of the first transistor-run computers in the world, the TX-0, was loaned to MIT, it was housed on the second floor of Building 26, and the model railroad club hackers were allowed to sign up for time to work with the machine, which was run around the clock. As their obsession with the TX-0 deepened, they began calling themselves "TX-0 hackers." They discovered that the best hours to book, or "vulture," time on the machine were in the middle of the night. First, you used a machine called a Flexowriter to punch the programming instructions into a long, thin paper tape, and then you fed those instructions into the TX-0. The TX-0 made sounds as you did so—a kind of low, out-of-tune organ music that changed according to the data the machine was reading. You could hear what part of your program was going through—that is, if you could hear anything over the din of your friends' clacking Flexowriters, "which would make you think you were in the middle of a machine gun battle."[4] You got the results of your programming immediately. For these budding pioneer programmers, the process was addictive.

The culture that coalesced around the model railroad club and the TX-0 hackers embodied precepts that, although only silently agreed on among themselves, would be distilled by Steven Levy into a "hacker ethic":

1. *Access to computers—and anything that might teach you how the world works—should be unlimited and total. Always yield to the hands-on imperative!* "Hackers," Levy explained, "believe that essential lessons can be learned

about the systems—about the world—from taking things apart, seeing how they work, and using this knowledge to create new and more interesting things. They resent any person, physical barrier, or law that tries to keep them from doing this."

2. *All information should be free*. "If you [don't] have access to the information you [need] to improve things, how [can] you fix them? A free exchange of information … [allows] for greater overall creativity."
3. *Mistrust authority*. *Promote decentralization*."Bureaucracies, whether corporate, government, or university, are flawed systems, dangerous in that they cannot accommodate the exploratory impulse of true hackers … [which these institutions] perceive … as a threat."
4. *Hackers should be judged by their hacking, not by bogus criteria such as degrees, age, race, or position*. "Hackers [care] less about someone's superficial characteristics than they [do] about his potential to advance the general state of hacking, to create new programs to admire, to talk about that new feature in the system."
5. *You can create art and beauty on a computer*. "Code … [holds] a beauty of its own." Among the TX-0 hackers, Levy explained, "A certain esthetic of programming style … emerged. Because of the limited memory space of the TX-0 (a handicap that extended to all computers of that era), hackers came to deeply appreciate innovative techniques that allowed programs to do complicated tasks with very few instructions."
6. *Computers can change your life for the better*."This belief was subtly manifest," Levy wrote. "Surely the computer had changed [these early hackers'] lives, enriched their lives, given their lives focus, made their lives adventurous. It had made them masters of a certain slice of fate."[5]

The professors who led the artificial intelligence (AI) work at MIT—Jack Dennis, John McCarthy, and Marvin Minsky—were early proselytizers of computers' potential to better the lot of the human race.[6] Minsky, more than others, understood the genius of the hacker approach and "encouraged hackerism in any way he could."[7] The "golden age" of hacking at MIT developed through the 1960s under Minsky's tutelage, with hackers like Bill Gosper, Richard Greenblatt, and Stewart Nelson joining the student ranks in the early part of the decade. This group of hackers worked on operating systems, programming language, distributed systems, and the theory of computation. They ate copious amounts of Chinese food, worked all hours, and led a monastic lifestyle. There were a few women programmers at MIT at the time, but they were not within the hacker ranks. Computing was then, and remains today, a

field dominated by Western white males. (This demographic is certainly a concern, considering computing's profound effects on society. It is not a direct focus of this book, although in the second half I show that as hacking proliferates and merges with social movements, diversity and inclusiveness are seeping into the field and beginning to have their effects.)

Soon, the MIT hackers began working with a much more exciting machine—the PDP series. Joseph Weizenbaum, author of the well-known ethical treatise *Computer Power and Human Reason: From Judgment to Calculation*[8] and an MIT student during this time, vividly described hackers' fevered lifestyle:

> Bright young men of disheveled appearance, often with sunken glowing eyes, can be seen sitting at computer consoles. … They work until they nearly drop, twenty, thirty hours at a time. Their food, if they can arrange it, is brought to them: coffee, Cokes, sandwiches. If possible, they sleep on cots near the printouts. Their rumpled clothes, their unwashed and unshaven faces, and their uncombed hair all testify that they are oblivious to their bodies and to the world in which they move. These are computer bums, compulsive programmers.[9]

The "golden age" hackers were even more hard core in their embrace of the hacker ethic than their TX-0 predecessors had been. Fighting the university bureaucracy to gain access to systems and tools, they developed a transgressive approach to rules. Richard Stallman, who came to the AI group at the tail end of this era, not long after Minsky established it as the "AI Lab" in 1970, recalled later in an interview,

> I don't know if there actually is a hacker's ethic as such, but there sure was an M.I.T. Artificial Intelligence Lab ethic. This was that bureaucracy should not be allowed to get in the way of doing anything useful. Rules did not matter—results mattered. Rules, in the form of computer security or locks on doors, were held in total, absolute disrespect. We would be proud of how quickly we would sweep away whatever little piece of bureaucracy was getting in the way, how little time it forced you to waste. Anyone who dared to lock a terminal in his office, say because he was a professor and thought he was more important than other people, would likely find his door left open the next morning. I would just climb over the ceiling or under the floor, move the terminal out, or leave the door open with a note saying what a big inconvenience it is to have to go under the floor, "so please do not inconvenience people by locking the door any longer." … There is a big wrench at the AI Lab entitled "the seventh-floor master

key," to be used in case anyone dares to lock up one of the more fancy terminals.[10]

SECOND-WAVE HACKERS: COMPUTERS AND CODE FOR THE PEOPLE, INCLUDING THE PEOPLE'S COMPUTER COMPANY, THE WELL, HOMEBREW, SILICON VALLEY, RMS, AND FREE SOFTWARE

As Levy observed, the impetus of this first wave of North American hackers at MIT was to "ingest the magic of the computer; to absorb, explore and expand [its] intricacies."[11] But through the 1970s, a second wave of hacking was gathering force in and around Berkeley, California, and a place called Silicon Valley in the southern part of the San Francisco Bay Area. It was marked by a much greater social consciousness and outward orientation than the early MIT hacker culture. The inspiration of this second wave of hackers was to *bring computers to the people*. Tech insiders will know this history well and might want to skip over it. But many ordinary computer users do not and will find it critical background for understanding contemporary hacking and digital tech issues today.

In the early 1970s, Intel began manufacturing the first computer microchips, spurring the dream that people could own small computers themselves. The People's Computer Company proselytized the democratizing power of the personal computer in a counterculture publication, a newsletter called *People's Computer Company* that gave heady dispatches from the front lines of the revolution, and also ran a computer center that offered classes and computer time to anyone interested for fifty cents an hour.[12] The Community Memory Project brought computer message boards to people in the streets of Berkeley.

The Homebrew Computer Club, another well-known group from this era of hackers, ended up realizing the personal computer revolution. It formed in 1975 to tinker with the first build-your-own home computer kit, the Altair (built using Intel's new 8080 microcomputer chip). The Homebrew enthusiasts came together in the spirit of the original hacker ethos to present new prototypes for each other's feedback, test each other's source code, and share solutions. Experiments and inventions were shared even with nominal competitors.

These second-wave hackers were forging their way on a new frontier together. "We reinforced each other," Lee Felsenstein, who belonged to both the Community Memory group and the Homebrew Computer Club,[13] later explained to Steven Levy: "We provided support structure for each other. We bought each other's products. We covered each other's asses, in effect. There we were—the industrial [IBM] structure was paying no attention to us. Yet we had people who knew as much as anyone else did about this aspect of technology, because it was so new. We could run wild, and we did."[14]

The conditions proved perfect for innovation. Within a few years, many of the Homebrew Computer Club's members went on to become major designers and manufacturers of personal computers, including Steve Wozniak, who designed the Apple I. The Homebrew Computer Club's hacker newsletter was a formative influence in the emerging culture of Silicon Valley, where the silicon microchip manufacturers and many of the startups in the personal computer revolution came to be located. These companies understood the power of the hacker ethic because it was in their DNA. They recruited hackers, modeled their work processes after hackers' processes, and loosened corporate culture to emulate a more freewheeling hacker culture.[15]

But the tension between the hacker ethos and the commercial, for-profit ethos soon created rifts. Back at MIT, one such rift opened up in the hacker scene when one set of MIT hackers started a company called Symbolics, developing proprietary code for a machine that ran Lisp software in competition with a project they had been working on with a larger group. By the end of 1981, many of the MIT hackers were employed by Symbolics and were working mostly at its offices instead of at the AI Lab, although they continued to be involved with MIT projects. Proprietary code cannot be shared outside of a company. It is a trade secret. By working for a competing company, these hackers had abandoned a key principle of the hacker ethic—the hands-on principle, the free flow of information.[16] A great deal of rancor was generated over the split, and rooms that used to be full of hackers working late into the night emptied. Steven Levy described the AI Lab in the mid-1980s as a place where the flame of the original hacker ethos still flickered but only barely. The professors, students, and nonhacker researchers at the lab did not know (and did not want to know) how to take the guts out

of machines and put them back together. The new programmers coming in did not want to tinker on things collectively. When they wrote new programs, they circulated them with a copyright notice, which was anathema to Richard Stallman. "I used to wander through the lab," he has said, "through rooms so empty at night where they used to be full and think, 'Oh my poor AI Lab! You are dying and I can't save you.' Everyone expected that if more hackers were trained, Symbolics would hire them away anyway, so it didn't even seem worth trying."[17] Stallman, Levy wrote, "grieved at the lab's failure to uphold the Hacker Ethic." He "considered himself the last true hacker left on earth."[18] "I'm the last survivor of a dead culture," Stallman told Levy.[19]

In fact, Stallman was a pivotal figure between the first wave and second wave of North American hackers. His instinct to rebel against any institution that would not make source code freely available for tinkering may have stemmed from the hacker's hands-on imperative, but Stallman, more than earlier hackers, was able to link this imperative to an outward-looking social vision, and he would pursue the implications of this for the rest of his working life.

In the early 1980s, Richard Stallman's inspiration was to *bring code to the people*. In January 1984, Stallman quit his job as a "system hacker" (developing software for MIT's operating systems) so that he could build a complete, Unix-like system that was "free." Unix was a widely used proprietary computer system in university computer science departments, and Stallman felt he could get the biggest uptake if he based his software on an interface already known to many people. He was compelled by his goals to quit MIT because if he had developed his software under MIT auspices, the institution could have claimed copyright on it and interfered with its distribution. A scientific atheist, Stallman has said the decision to start his project was prompted by the same altruistic spirit expressed in the famous aphorism attributed to the religious leader Hillel: "If I am not for myself, who will be for me? If I am only for myself, what am I? If not now, then when?"[20]

He called his software "free," explaining that he meant "free as in freedom, not price." Stallman had no problem with people selling free software, which might be necessary to make a living or fund development projects. To be "free software," he held, software had to comply with the "four essential freedoms." Users had to be

0. Free to run the program as they wished, for any purpose;
1. Free to modify the program to meet their needs, which entailed access to source code;
2. Free to redistribute copies, either without charge or for a fee; and
3. Free to distribute modified version of the program so that the community could benefit from one's improvements.[21]

Stallman's answer to the question "Who controls code?" was definitively "The user."

Stallman sent an open email to the unix-wizards listserv:

> Starting this Thanksgiving I am going to write a complete Unix-compatible software system called GNU (for Gnu's Not Unix), and give it away free [at no cost] to everyone who can use it. … I may be able to hire a few people. … The salary won't be high, but I'm looking for people for whom knowing they are helping humanity is as important as money … So that I can continue to use computers without violating my principles, I have decided to put together a sufficient body of free software so that I will be able to get along without any software that is not free [in the sense of the "four freedoms"].[22]

Stallman and his collaborators made a list of the programs needed to make a complete operating system, including command processors, assemblers, compilers, interpreters, debuggers, text editors, and mailers. Then they systematically "found, wrote, or found people to write everything on the list."[23] As his recruitment email stated, he called it GNU (Gnu's Not Unix), a recursive acronym, the kind of joke that hackers like. In 1985, Stallman published "The GNU Manifesto," a declaration of his intention, and started the Free Software Foundation, a charity for the development of free software.

FIRST-WAVE EUROPE: THE EARLY DEVELOPMENT OF EUROPEAN HACKER CULTURE IN THE 1970S AND 1980S

In Europe, hacker groups like the Chaos Computer Club developed later than hacker culture in the United States and not always with much consciousness of US hacker culture. The dawning of hacker culture in Europe aligned more with the advent of personal computing than with the development of early mainframe computing.

By the late 1970s in Europe, personal computers were beginning to enter people's lives, and governments there and in the USSR were promoting the technology, encouraging computer literacy in their populations with a range of initiatives. To bolster national economies in the slump of the 1980s, several governments supported the development of national computer industries, but these efforts were largely unsuccessful. Government support for Dutch Tulip, Swedish Compis, Yugoslav Lola, and Polish Meritum, for example, was insufficient for these companies to keep up with the rate of innovation by US companies.[24]

People on both sides of the Iron Curtain were embracing, experimenting with, and appropriating computer technology within their own political and social contexts. The user manuals were not necessarily published in their languages, and there was room and a need to experiment with the basic programming that came with commercially distributed computers.

In the Netherlands, computer tech was embraced quickly by a civic-minded, hobbyist culture. In Greece, where the early, Western-built gaming and personal computers provided nothing to help users adapt them to the Greek language, hacking software was imperative and became the norm. In Yugoslavia, which was an autonomous Communist state wedged between the USSR and Europe, the government promoted an autonomous, national computer industry, and the thriving hacker scene there was elitist rather than being motivated by counterculture politics.[25] Behind the Iron Curtain, Polish hackers had access to computer magazines and grassroots publications and maintained connections with clubs and periodicals in the West, despite Cold War restrictions. Also behind the Iron Curtain, Czech hackers, lacking a WiFi infrastructure, experimented successfully in sending beams of light containing data to each other. Usually red, these data beams could be seen stretching eerily across apartment-building courtyards and Prague rooftops at night. In Finland, the socialist culture that produced both Linus Torvalds (the instigator of the collectively produced Linux kernel) and the Angry Birds game, many hackers were part of a "demoscene" that treated hacking as a form of real-time, collectively produced art, creating "demonstrations" out of hacks of popular computer games. In France and Italy, politically conscious hacker groups sprang up that were aligned with the republican and anarchist traditions of those countries.

THE EARLY DAYS OF THE CHAOS COMPUTER CLUB

In Germany, yet another very specific set of social and political circumstances shaped hacker culture. In the 1970s, West Germany was still divided from East Germany, which formed part of the Communist bloc. West Germany had gone through the counterculture politics of the 1960s with the rest of Europe; East Germany had not. West Berlin was not contiguous with the rest of West Germany but was an island of heavily fortified democracy that had been saved from the encroaching Soviet army by the Americans' Berlin Airlift at the end of World War II. It was entirely surrounded by Communist East Berlin.

In Hamburg, West Germany, Wau Holland imbibed the ideas of the 1968 student revolution, which had erupted in international protests against state authority. He was anticapitalist, antistatist, and somewhat anti-American. He had studied electrical engineering, computer science, and politics and then worked in leftist bookstores for a while. But his ideas did not fit well within the leftist spectrum of the era. In Germany, countercultural movements had, for the most part, adopted a skepticism toward technology influenced by the Frankfurt School and were wary of technophiles.

Holland, having "no natural audience on the left … had to create one himself."[26] He felt the Green Party, for example, fought technological developments "with garlic, the cross and holy water."[27] In an instrumentalist, technology-driven world, he believed one should fight back with technology, humor, and ethics. It was a strategy he called "positive chaos."[28] His take on tech was somewhere between the utopian vision of the People's Computer Company in California, which saw computers as innately liberating and democratizing, and a more anarchist appropriation. In an influential article he published in the newspaper *Die Tageszeitung* (*taz*) in 1981, he invited fellow computer enthusiasts to "stop scurrying around" and meet with him to discuss important issues like data laws, encryption, and copyright. He convened a regulars' table at a local alternative bookstore.

In 1982, in *taz*, he announced the formation of the Chaos Computer Club. With its technophile bent, it diverged from conventional counterculture thinking, but the Chaos Computer Club was still, from its inception, a counterculture group. It is no coincidence that the Kommune

1 table, around which its inaugural meeting, real or apocryphal, was held, became the club's chosen transgressive icon—an object associated with a 1960s counterculture group so notorious in Europe that hackers thrilled to imagine what might have been done at or on top of it.

I did not ask Andy if he had ever been photographed at that table in a hagiographic image of club founders, but he most certainly got involved with the club around the time it began putting out its influential newsletter, *Datenschleuder*. After Holland announced the publication of *Datenschleuder* in *taz* in 1984, he immediately received a hundred advance orders. The publication was a hodgepodge of technical discussion, disclosures, political disquisition, and announcements of new projects. The group became a self-identified "vanguard" of the information society, and its preoccupations were state and corporate accountability, consumer protection, user empowerment, and a 1968-era concern about struggling against centralized, opaque systems, whether political or technical. Among its many outreach actions, the club showed people how to build their own modems, exposed security vulnerabilities, released the technical specifications for broadband networks and government protocols for shutting down telecommunications in times of emergency, and after the nuclear reactor meltdown at Chernobyl, discussed a project for monitoring radioactivity using personal computers.

Anyone could subscribe to the newsletter, but in order to become a member of the club, one had to demonstrate both technical prowess and playfulness: the entrance requirement was to program a "quine." A quine is like a recursive joke but in programming code. It is a piece of code that refers to itself in a way that causes it to keep reproducing itself. There is, in fact, a "recursion theorem" in programming (Kleene's) that "proves the existence of quines in every sufficiently strong programming language," but they are not easy to discover.[29]

In 1984, Holland and Steffen Wernéry, an important collaborator of Holland's and spokesperson for the Chaos Computer Club, announced the hack of the Bildschirmtext (Btx). The Btx was an early teletext system offered by Germany's federal mail service and main telecommunications provider, Deutsche Bundespost (DBP). The club had repeatedly warned the DBP that the Btx system was flawed. Btx had been introduced to a public that was already wary of large, opaque technical systems: West Germans had protested against nuclear energy production and

against the 1981 population census, finally winning a novel right to "informational self-determination." The club did not like DBP because it held a government monopoly over telecommunications and controlled access to the system, including what kind of hardware could be used legally.

DBP ignored the club's repeated warnings and denied there were weaknesses in Btx. By hacking emails, the club discovered Btx users' passwords and began publishing them. Provoked into stronger action by DBP's dismissals, the club found the password for Hamburg's savings bank, Hamburger Sparkasse (HASPA), and used it to transfer 135,000 deutschmarks (DMs) to the club's bank account in just one night. The money was returned the next day, and Holland and Wernéry held a news conference to report the "robbery" to Hamburg's data protection commissioner.

The hack was the kind of performance politics Kommune 1 would have appreciated and a demonstration of the club's evolving tactics of "countercontrol" and "inverse panopticism." The BDP accused the hackers of malfeasance, but the media and public applauded.

Although at first the club's "hacktivist" stunts were received favorably by the public, by the late 1980s, the fleeting positive image of hackers that CCC had helped create was overtaken by news stories of very young hackers doing reckless stunts and cracking systems without much, if any, coherent political thought. The public's view of hackers as defenders of the public interest began to change. Increasingly, they were seen as trespassing hobbyists with dangerous criminal proclivities that the state was obliged to protect the public against. A series of high-profile attacks on US military complex targets—culminating in the "WANK" worm attack on the National Aeronautics and Space Administration (NASA) and contemporaneous attacks on EU targets—brought things to a head. In Europe, the hackers had apparently used a flaw in the VAX system, which was used by public authorities to access the computers of research facilities and companies. Companies alleged the hackers had copied and destroyed data in over a hundred machines. The perpetrators, out of their depth, anonymously contacted the Chaos Computer Club for help.

What assistance, if any, was given to these anonymous troublemakers, Andy might be able to tell. What is known publicly is that the club

notified Germany's Federal Office for the Protection of the Constitution. Law enforcement agencies began a preliminary investigation to determine the hackers' identity. Other jurisdictions became involved, and Steffen Wernéry became one of the suspects. The media coverage against the club was harsh.

In 1987, there was a police raid at the club's Hamburg headquarters. When Wernéry was traveling to Paris in 1988 for a computer conference, he was arrested for computer crimes.[30] He was later released back to Germany after serving two months in a French prison for hacking the the code of the Dutch electronics multinational, Phillips.[31]

1989: A WATERSHED YEAR FOR GERMANY AND THE CCC

As Andy tells it, 1989 was a big year not just for Berlin and Germany but also for the Chaos Computer Club. In March 1989, nine months before the fall of the Berlin Wall, the KGB story broke.[32] Some youths affiliated with the club had hacked into computers in the US and EU and transferred source code and other documents to the KGB for money.

The KGB hack was a complete breach of what Wau Holland and others in the club considered "a decent way of hacking."[33] It created a big commotion within the European hacker community and forced the club to face the problem of dealing with its own wayward teenagers.

This was also the year of the first big international hackers' meeting, held in the Netherlands at the Paradiso, a large church converted into a meeting hall.[34] At this seminal gathering of hackers from all over the world, especially the US and EU, Wau Holland took the opportunity to make an example of the kids involved in the KGB hack. He pulled one of them up and conducted a public interview with him for the edification of everyone at the conference. It was an important moment in the oral, and moral, history of the hacker scene.

The fact that European hackers still talk about and recreate the event is indicative of the special influence Wau Holland and the Chaos Computer Club have exercised in the European hacking scene. In the interview, a transcript of which still exists,[35] Holland underlines the hacker ethic to which the CCC is committed. Like an Old Testament father figure, he lays down the principles in full for the eighteen-year-old, who went by the code name "Pengo." The principles Holland recites are the original

hacker precepts distilled by Steven Levy in his book *Hackers: Heroes of the Computer Revolution*.

In the interview, Holland tells Pengo and the audience that he is angry and disappointed and that hackers need to trust each other. "We as hackers should be guided by a hackers' ethic as it was described in the 1984 Hackers Convention," he says and proceeds to enumerate the Levy list:

Number 1: Access to computers, as with anything that can teach you how the world works, should be unlimited and total. Always cling to the hands-on imperative.

Number 2: All information should be free.

Number 3: Distrust authorities, and promote decentralization.

Number 4: Hackers should be judged only by their hacking, not by bogus criteria such as age, race, position, or degrees.

Number 5: You can create beauty and art on a computer.

Number 6: Computers can change your life—for the better!

Holland tells Pengo and the audience, "I'm not saying that the hackers' ethic is an iron law; hackers always break laws, even their own, but what Pengo did was ignoring them altogether."

In the interview, Pengo himself confesses that, looking to make a profit, his group contacted the KGB with the expectation that an intelligence service would be interested in hacker knowledge and that thrill-seeking had led them along:

> Intelligence services have always been interested in computer knowledge. And we thought of ourselves as the most ingenious people in the world so we didn't bother too much to question for which people we were working in the end.
>
> At first we penetrated computers and didn't see the social consequences of our actions. Fascination with technology led more or less to fascination with power. Breaking into computers was a more or less ethereal pleasure. Making contact with this KGB agent was total life, very real indeed. Suddenly I became the star in an espionage movie. Hacking was just playing with a toy, contacting the KGB agent was real social interaction. Everything was a swirl.

"Well, you crossed the threshold you shouldn't have crossed," Wau Holland tells him: "You started out playing a game that you were too young to play, and now you are part of a game that secret services play,

you are their prisoner … and if you don't have your own strong ethical standards, you will remain their plaything."

"It's an old question," Holland tells the hacker audience: "Who profits? Every time I deal with information, I have responsibilities. I can kill people with information. We've been thinking about this in the Chaos Computer Club. You can, for example, break into the control computer of an atomic reactor and provoke a catastrophe."

"Isn't that somehow fascinating?" the incorrigible Pengo interjects, and Holland continues resolutely:

> Yes, it is. But fascination is dangerous because you might not see the existing limitations. The Chaos Computer Club is not just a bunch of techno freaks: we've been thinking about the social consequences of technology from the very beginning and I think our strength derives in part from our moral standards. Everybody must face the question "What am I doing?" … We Germans already have such a bad reputation that one really couldn't be careful enough.

Driving fast down the Autobahn, Andy tells me that Pengo's group of young hackers was manipulated by criminal elements "who thought it was an easy deal to deliver these kids up, with their abilities, to people who had a use for them." There's a lull in the conversation as I take in this information. "That local hacker group seems to have had a lousy set of morals," Andy adds over his shoulder without taking his eyes off the road.

Not long after the Paradiso interview—on May 23, 1989—a body was found in a forest near Hanover. It was Karl Koch, a hacker from Pengo's group.

"He was found burned in a forest with his shoes and car keys removed and in bondage," Andy says. "But I'm sure you don't want the gory details. Officials said it was suicide. The case was never investigated." He shrugs. "He got in between German Interior Department, American, and Russian interests."

"The second time a kid got killed," Andy continues, and I hunch forward from the back seat now to be sure to catch his words, "I thought it was my duty to find out what had happened. You know, crying parents, and with such an event happening you have people who get scared.

It's not sexy. They come to play with their tech and then start to run away."

The second kid was a young hacker who went by the handle Tron and specialized in smart cards and video encryption. In 1998, he came under the influence of piracy groups, a situation that ended badly. "The same methods used to secure encrypted TV are also used to secure military satellite communications," Andy explains. "He was too young to understand the impact of his technology.

"At one point, a friend told us, 'You guys have a choice. You can either fall within the definition of a criminal organization, or you can incorporate.' So we became a limited liability, registered association."[36]

THE FALL OF THE WALL

A few months after the KGB affair broke, in November 1989, the Berlin Wall came down.

Many East Berliners put aside their daily undertakings and, taking no chances, walked straight over to West Berlin, leaving whole neighborhoods empty in East Berlin. The flux went the other way, too. The artists came from West Berlin into East Berlin right away. So did people like Andy.

It was chaotic, and the infrastructure was crappy. Some neighborhoods, like Spandauer Vorstadt, were in such bad repair that they were pretty much completely deserted. Some 130 buildings in East Berlin were occupied by squatters, mostly young people who created their own unified Germany before formal reunification in 1990.[37] The slogan "Wir sind das Volk" (We are the people), which was chanted at the GDR protests, quickly became "Wir sind ein Volk" (We are one people).[38] The graffiti that had been restricted to the west side of the Berlin Wall spread like a virus into East Berlin. It is still one of the most ubiquitous features of the urban landscape there.

This new squatter movement in Germany was in synch with a hacker group like the Chaos Computer Club, which played with the idea of ownership in the sphere of digital tech and tested notions of private property, equal access, and shared use. The Dutch slang word *kraken*, coined to mean both hacking and squatting, pointedly fused the physical and the cybersphere claims to common goods.[39]

A newly constituted version of the Chaos Computer Club also fused East and West. "The Chaos Computer Club became two groups melded," Andy explains: "A group from East Germany and a few guys, including me, from the West German hacker scene. The East German guys had their own way of dealing with reality and intelligence. The great news about the whole situation was, when the Wall fell, we had the most complete disclosure for any security agency on earth. The Stasi was the best documented security agency in history, and we had access to all their manuals, like 'How to Bring Distrust into Groups' and 'How to Destroy Political Movements,' and we discussed all these things in the club. If you look at what happened to Julian [Assange], it's in the manuals. So in the CCC, we have a bit of immunity from totalitarian structures in our attitude."

A good friend of Andy's, Wolfgang Kaleck—the person who arranged my ride with Andy to the camp—also came to East Berlin at that time. A criminal lawyer straight out of law school, Kaleck arrived in East Berlin to set up a small progressive law firm. The young lawyers tried to bring Stasi members to court, but it was difficult because the worst abuses—including torture—had happened decades earlier.

THE 1990s: HACKERDOM EXPANDS, SILICON VALLEY TAKES OFF, AND A SCHISM DEVELOPS BETWEEN THE PHILOSOPHIES OF PROPRIETARY SOFTWARE AND FREE SOFTWARE

In the United States in the 1990s, the question of who controls code, posed by Richard Stallman in 1983 with his launch of the free software movement, evolved into a philosophical schism. It is a schism well known to tech insiders, and ordinary computer users need to understand it, too.

In 1991, not long after the tumultuous events of 1989, Tim Berners-Lee launched the World Wide Web. By 1995, Berners-Lee's invention had become widely embraced by the public, and the internet as most people know it was born.

The internet brought hacker groups across countries into closer connection. The different scenes became even more aware of the statements and manifestos of their counterparts, especially across the Atlantic. Hackers developed a more unified, self-conscious philosophy and a shared language. To be sure, there were diverse lineages and strains

of hacking: the origin story of hacking is more complicated than Levy made it seem, and his articulation of a singular hacker ethic was not adopted by all groups.[40] But ideas began to diffuse internationally, and important international relationships were built. Levy's articulation of a hacker ethic, as mentioned earlier, was adopted verbatim by the Chaos Computer Club,[41] and its tenets and the tenets of free software spread widely throughout the scene coalescing around CCC events.[42] At the same time, social activist groups began using the internet to organize and communicate, and the global social justice movement was built. A new net culture emerged, along with the ideas of digital rights and net citizenship.

The hacker world was expanding everywhere in the 1990s, in tandem with the spread of personal computers. The decade saw a proliferation of hacker fanzines, conferences, hacker spaces, and hackathons.

But by the 1990s, hacking was a complex terrain. Richard Stallman's "free software" principles profoundly influenced how the internet and then the World Wide Web were built and left unenclosed for anyone to use. At the start of the decade, around the same time the World Wide Web was invented, Stallman won a MacArthur "genius" award in the United States.[43] Someone was paying attention. In 1992, hackers in California, John Gilmore (a founding member of the Homebrew Computer Club) among them, founded the Electronic Frontier Foundation, an early advocate for users' rights and for the defense of hackers when they tangled with the law.

At the same time, digital tech by the 1990s was well on its way to becoming a multi-billion-dollar industry. The halcyon hacking days of the Homebrew Computer Club had been short-lived. Started in 1975, the club reached its peak in 1977 with the West Coast Computer Faire, an event Steven Levy called the Woodstock of the burgeoning California hacker scene.[44] Hundreds of people were still coming to the club's meetings, and fifteen thousand subscribed to its newsletter, but the core members who had gone on to start companies stopped attending and began to focus on their bottom lines, recreating the club culture within their own staffs and keeping their ideas to themselves. Silicon Valley giants like Apple incorporated the hacker ethic into their identity and production processes, understanding that the obsession, mastery, and collective problem solving of hackers were keys to their success. A

proliferating startup culture also celebrated the hacker identity. But by the 1990s, the California computer culture had become deeply invested in secret, proprietary software and hardware.

Meanwhile, Richard Stallman, stalwart in his hacker ideals, ploughed on. By the early 1990s, GNU developers had put together a whole integrated operating system of free software, except for the "kernel," which is the program at the center of the operating system that allocates the machine's resources. In another large collaborative process, Linus Torvalds, the Finn, was working to create a kernel that could serve a modular system.[45]

In 1992, the Linux kernel was freed through a free software license (Richard Stallman's GNU General Public License, version 2, otherwise known as the GPLv2) that guaranteed free software's "four essential freedoms" for users. The story of the kernel's development, its founding developer Linus Torvalds, and its mascot (the Linux Penguin) are all widely known to most computer users. GNU's story is less well known, and its mascot (a geeky gnu) is perhaps not as cute as the penguin. Like the incredible incubator of the Homebrew Computer Club, both of these projects showed what could be achieved with open, collaborative hacker efforts and have since become widely studied precedents of cooperative processes.

Richard Stallman has said, "By the time Linux was started, Gnu was almost finished." It was good timing because by the time the GNU network of contributors got to the final step of developing the GNU kernel, called "Hurd," it had encountered technical difficulties. In the spirit of free software, users started putting together the GNU system with the newly available Linux kernel, and Stallman called the complete system GNU/Linux.[46]

GNU/Linux took off with users and programmers due to its clear practical and technical advantages over proprietary systems. But much to Stallman's chagrin, most people began referring to the GNU/Linux system—the first complete free software operating system in existence—simply as "Linux." As Stallman is at pains to reiterate, only the kernel was Linux. To add further confusion, users persisted in thinking that *free software* meant "without charge." Proponents' efforts to keep explaining that *free software* meant "free as in free speech, not as in free beer" did not seem to make much of a dent in popular understanding.

Throughout much of the 1990s, the two cultures—one of "proprietary" code and the other of "free software" code—coexisted without much overlap. Although tech companies had embraced hacker culture in the service of product innovation, they were wedded to the idea that secret, proprietary software was the best way of making a profit, and the hacker ideal of "free software" was not an obvious value proposition to them.

Then in 1997, Eric Raymond's essay (later turned into a book) "The Cathedral and the Bazaar" was published. Raymond's thesis was that "given enough eyeballs, all bugs are shallow." He called this "Linus's law." He argued that the more widely a program's source code was made available for scrutiny and tinkering by users, the faster its flaws could be discovered and fixed, and the more robust the program would become. By contrast, in a "closed," proprietary model, where only a few company developers had access to the code, it would take an immense amount of time to look for bugs, and the program would be less optimized.

Put to them as a commercial proposition, companies came around to embrace the idea. "Open source" became an important mode of commercial production. Meanwhile, companies and government agencies were also discovering the quality and versatility of free software products. GNU/Linux became ubiquitous. The Linux kernel became famous for its reliability and stability. It was widely recognized for its capacity to work on any chip in the world and manage the demands of many software programs at once.[47] NASA replaced large parts of its proprietary software with versions of GNU/Linux.[48] The Linux kernel was used by Google for the heart of its "Android" operating system (which by 2016 would corner 85 percent of the market share for smartphones, vastly more than Apple's iOS operating system for the iPhone).[49] Eventually, GNU and the Linux kernel would run on most of the internet's servers, on most of the world's supercomputers, on the New York Stock Exchange, and on the platforms of Google, Facebook, and Amazon. The US government would use the Linux kernel. It could found running on medical equipment, on drones, on warships, and in the burgeoning Internet of Things.[50]

Richard Stallman considered "open-source software" a cooption of the free software movement's work and a rejection of its values. As a product, he has said, open-source software is usually equivalent to free software (there are some licenses, not widely encountered, that qualify as open

source but not as free software because of restrictions they contain), but it is amoral.[51] It adopts free software's method of development but drops its philosophy. It is not motivated by a commitment to freedom and giving users full control over their computing.

Today, there are many "distributions" (curated collections of programs) that contain "free" and "open source" and "closed proprietary" software together, and companies have donated significant amounts of money to further the development of the free Linux kernel. But the fact that most distributions with free software components also contain software components that are not free deprives users (including government users) of full control over their computing. Another practice, known as "tivoization", which locks up free software inside unfree software so that it cannot be accessed and modified, deprives users of the benefits of the free software altogether.

Stallman has tried to get at this last practice with a new license, the GPLv3, which adds a prohibition on tivoization, in addition to guaranteeing users the "four freedoms," but adoption has been uneven. (The point of the GPLv2 is to make middlemen pass along the "four freedoms" to end users. GPLv3 extends this by banning them from tivoizing.) Linus Torvalds has rejected the GPLv3 license for the Linux kernel. And recently, Google has threatened to remove the free Linux kernel at the heart of its Android operating system. It might replace it with a new open source kernel called Fuchsia, but without GPLv2 or GPLv3 protection, so that manufacturers will be allowed to make the versions they ship totally proprietary.[52] If this happens, there will be no smartphone device on the market that users can modify and control as they wish.[53] (Currently, five out of six of the leading smartphones on the market are powered by Google's Android operating system.)[54] Some people in the free software movement are complaining that companies leach the expertise of hackers and fail to pay back to the community by following the free software philosophy.

So "open source" or "open code" is *not* the same as "free software" or "free code." It is ironic that a man who wanted code—computer language—to be in the control of users has had his advocacy efforts frustrated by the semantics of the English language. Unfortunately, the ideas behind free software are simply more complicated than a single word or name can fully denote. Stallman is constantly trying to untangle the

confusion: Linux was *not* the complete operating system that started the free software movement; free software does *not* mean software given away at no cost; open-source software is *not* the same thing as free software.

Even by the 1990s, it was becoming apparent that the world was being built with code. The microchips that ushered in the personal computer revolution had led to ubiquitous computing. Computer systems were not just sitting on people's desks; they were in everything. For those who reflected seriously on it, Stallman was a visionary in a world in which code was coming to control everything. His implicit question, "Who gets to control code?" was hugely significant.

In that light, Stallman's promulgation in 1985 of his GNU manifesto was a seminal moment. It marked the beginning of a great schism between free code (in the user's control) and proprietary code (not in the user's control) that now looms over the digital age in the twenty-first century.

Hackers and a few academics like Harvard's Larry Lessig understood the significance of Stallman's GNU manifesto. In the hacker community, the idea of free software would become as important an organizing principle as "liberty, fraternity, and equality" was for early Enlightenment democrats. In fact, free software is arguably the digital age descendant of those principles, if twenty-first century democrats could only realize it.

We've left the Autobahn and have been driving past tidy farmhouses built in the old style but with brand new materials. Their red roofs are glossy, and the whitewash fresh. A field of giant wind turbines comes into view on the slope of a hill ahead, their massive propellers circling gracefully.

I feel the pressure of trying to cover the whole hacking landscape in whatever interviews I can get over the next few days at the camp. I'm not an academic researcher with the luxury of time and the constraints of a discipline to help me—I must focus on what is most salient to my concerns as a citizen. I've been reading about revolutions lately in research for this book, and I think about what the Russian revolutionary Leon Trotsky once said about the German Social Democratic leader Ferdinand August Bebel. Bebel, Trotsky said, "personified the slow and stubborn movement of a new class that was rising from below … a class that gets its learning during its spare hours, values every minute, and absorbs voraciously only what is strictly necessary."[55] I am comforted by the thought

that this might be as valid an approach for attacking an urgent political subject as any more circumscribed, academic method.

I wonder out loud what the present state of hacking is in the United States and in Europe. Where are the true hackers now? Where do hacker scenes even exist?

Andy glances in the rear-view mirror and changes lanes to avoid some roadwork. "The Chaos Computer Club France was run by a snitch until we found out and intervened. La Quadrature du Net is an important group. The Spanish are getting stronger. There's a small hacker scene in Switzerland and Austria. Italy and Holland are important. In the UK, there's no political space, and no culture for it. Their Parliament just voted in the worst of the worst cyberlaws."

And in the US?

"It's all commercialized there now," Peter says. "Defcon is a corporate event. Europeans don't think much is going on in the US now that's important, either politically or technically. Especially at the Defcon and the Black Hat conferences. These are the same people. They will sell their wares to anyone who pays. They had General Keith Alexander give the keynote at the Defcon conference in 2014!"[56]

Andy says, "John Gilmore [founding member of the Homebrew Computer Club and the Electronic Frontier Foundation] has always been about taking care of society—although John got a little afraid around the WikiLeaks stuff and backed off, maybe because he was surrounded by a bunch of anxious lawyers. Then you have the 2600 crowd,[57] who have not talked to each other in twenty years, and they are heavily infiltrated. They think it's okay to tell each other funny tech stories and don't mind if someone is a spook."

So is the Chaos Computer Club a leader when it comes to progressive hacking?

Andy is quick to squelch the idea that the Chaos Computer Club is a leader: "You're using a term that we can't accept. We don't like leaders. Yes, we like progress and people making cooperation, but go away with 'leaders.' I like the idea, rather, that we provide spaces where things can happen. The motto is to 'Always act in a way where you widen the options to act.' And the CCC has managed to provide a space where young people can learn and discuss things. But to be blunt, I wish the young people were more political than they are. You shouldn't put us up as heroes."

"Yes," Peter says. "How are we going to save the world when we also have jobs from nine to five, just like everyone else?"

FIRST IMPRESSIONS: BE EXCELLENT TO EACH OTHER

We've been driving on back roads through the countryside for a while now, the houses getting sparser, until finally we go down a long road and pull into a large, dusty parking lot with masses of tents pitched beyond it as far as one can see. The rest of our conversation is cut short as we climb out of the car, stretch, and survey the camp.

This year the Chaos Computer Club's Chaos Communication Camp is being held at the site of a large nineteenth-century factory that once supplied Berlin with its terracotta roof tiles. As we approach the box office gate, Andy and Peter, smiling wryly, say I'll have to argue for myself to get in. "Use anything you think might help you," jokes Peter. I walk over to the plywood ticket booth, ready to say I've just arrived with Andy, but they seem to have a policy that anyone who arrives at the gate can buy a day pass at a premium price. So I'm in, with only my wallet compromised.

Andy has meetings to attend, and I wander off into the camp unchaperoned.

It is vast and it looks chaotic, but in fact it is wonderfully organized. An elaborate electrical grid has been laid down along the dusty ground over the whole area of the camp, which covers about twenty acres. The grid serves the "hacker spaces"—large white tents open at all hours and filled with desks and outlets for hackers to congregate around. It serves the giant circus tents that are the main speaking venues for the camp's extensive and varied event schedule, and it serves the sparkling food tents that glitter in copses of trees, each with its own whimsical decorations, from the Töller paintings of the handmade-latke restaurant to the cutlery and teacups dangling from tree branches surrounding the vegan kiosk.

The electrical grid serves the "national" tents, sporting flags of Norway, Italy, and France, and it serves the warren of squares and stages rigged up by superkeen engineers who have spared no effort in building out their environment. It powers the wacky experiments on display here and there—from a computerized crêpe-flipping machine to gizmos lining the pathways surrounded by beer-drinking comrades who laugh and cheer on

the people struggling to make their inventions work. The grid lights the friendly bars that look like the festive bars at tropical resorts and, always nearby, the huge caravan tents with multiple peaks sheltering homey arrangements of living room furniture, usually matching, including large white Naugahyde sectionals, orange sofa-and-recliner sets, and tasteful brown ensembles. And it powers the consoles where hackers are creating techno music on the spot. (Andy has told us the camp uses forty-five tons of sofas and loveseats, which the club stores during the four years between events, giving some idea of the effort that goes into staging them.)

The thick electrical cables are covered at crossroads, where bikes and baby buggies pass over them. A trolley train runs over the old tile factory's internal railroad tracks, trundling smiling families, bathers with towels around their necks, and gaggles of drink-sipping campers to where they want to go. There is a delightful small lake, I discover, where, from the fresh early morning until the silken hour of dusk, people and dogs jump into the water from docks and rafts. There are large tent villages, and someone tells me, "No one tells you where to put your tent. You just have to work it out with your neighbors." A couple of main arteries, wider dusty roads, divide the camp into quadrants.

There is something sweetly ingenuous about hacker culture. Small signs are affixed to tents that say "Be excellent to each other," a motto from the Keanu Reeves time-travel movie of the early 1990s, *Bob and Ted's Excellent Adventure*. Camping has never been this comfortable or convivial. You can strike up a conversation with anyone. Hackers don't make judgments about who you might be based on signs of status, your age, or your looks; they wait to see what you might say or do. The outdoor bars serving beer and the hackers' energy drink of choice, Clubmate, are staffed by charming people. Everyone brings their bottles back, there is no trash problem, even the washrooms stay orderly. People are indeed excellent to each other.

Photographs are forbidden, but it's hard not to want to take them because the light displays are beautiful. The techno music is entrancing. The camaraderie so apparent. The camp radiates a collective intelligence. It is a hive of peaceful, collaborative activity, like a science fiction vision of what the future with technology could be. There are a few families with children. It is mostly men, but there are many women too.

As dusk falls, the big rocket ship (yes, there is a fifty-foot-high mock-up of a rocket ship) is glowing and pulsating light in the middle of a large field, and people are relaxing and dancing around it.

The whimsy of it all reminds me of an early note of Julian Assange's, written by him in around 2007 to recruit students to his WikiLeaks project. Assange had been one of those teenage hackers (described earlier) who gave hackers a bad name in the 1980s. He joined the hacker underground in Melbourne and, with a group that included two other young hackers, conducted that series of cyberattacks against US and EU targets which were reported in newspapers in Germany.[58] *His* was the teenage hacking group that likely contacted the Chaos Computer Club for help in the late 1980s. After Assange was criminally charged, it took five years for his case to be finally resolved, in 1996.[59] The judge let him off with a fine, and he had gone back to school, attending Melbourne University's Math and Statistics Department, where he served as the puzzle master for a traditional start-of-academic-term treasure hunt.

A year after leaving the university, he used the school listserv to write the following note:

> Dear Puzzle Hunters …
> Are you interested in being involved with a courageous project to reform every political system on earth—and through that reform move the world to a more humane state? We have only 22 people trying to usher in the start of a world-wide movement. We don't have time to reply to most reporters' emails, let alone the interview requests—and I leave for Africa in under a week! We need help in every area, admining, coding, sys admining, legal research, analysis, writing, proofing, manning the phone, standing around looking pretty, even making tea.[60]

It was the start of a brave new adventure that would cast hackers as central characters in the struggle for democracy in the twenty-first century.[61]

NOTES

CHAPTER 1

1. See "Reichstag, New German Parliament," Foster + Partners, Berlin, Germany, 1999, http://www.fosterandpartners.com/projects/reichstag-new-german-parliament.

2. In 2016, the number grew to twelve thousand people. Darko Janjevic, "Chaos Computer Club: Europe's Biggest Hacking Conference Underway in Hamburg," *DW*, December 28, 2015, http://www.dw.com/en/chaos-computer-club-europes-biggest-hackers-congress-underway-in-hamburg/a-18944610.

3. Steven Levy, *Hackers: Heroes of the Computer Revolution* (Sebastopol: O'Reilly, [1984] 2010). Some hackers do not ascribe to the ethic as articulated by Levy, and there are many academic studies on the diversity of hackers. Some of the academics working in this field include Goetz Bachmann, David Berry, Jessica Beyer, Paula Bialski, Finn Brunton, Anita Say Chan, Gabriella Coleman, Laura DeNardis, Marco Deseriis, Ricardo Dominguez, Joan Donovan, Tor Ekeland, Virginia Eubanks, Karl Fogel, Felipe Fonseca, Volker Grassmuck, Christina Dunbar Hester, Benjamin Mako Hill, Matthew Hull, Matthew Jones, Tim Jordan, Christopher Kelty, Beth Kolko, Sebastian Kubitschko, Lawrence Liang, Sylvia Lindtner, Geert Lovink, Fenwick McKelvey, Colin Milburn, Luis Felipe Murillo, Lily Nguyen, Whitney Phillips, Matt Ratto, Thomas Rid, Renee Ridgway, Andrew Russell, Molly Sauter, Rebecca Slayton, Johann Soderberg, Felix Stalder, Ravi Sundaram, Yuri Tahkteyev, Douglas Thomas, Fred Turner, MacKenzie Wark, Sarah Meyers West, and David Murakami Wood.

4. Levy, *Hackers*, 16–17.

5. Levy, *Hackers*, 28–34.

6. Levy, *Hackers*, 57.

7. Levy, *Hackers*, 48.

8. Joseph Weizenbaum, *Computer Power and Human Reason: From Judgment to Calculation* (San Francisco: W. H. Freeman, 1976).

9. Weizenbaum, *Computer Power and Human Reason*.

10. The Cyberpunk Project, http://project.cyberpunk.ru/idb/hacker_ethics.html: "The Cyberpunk Project (TCP) is a remotely available data-well net of files about cyberpunk subculture, cyberpunk science-fiction and general cyber culture in the form of collected information. It is the result of years of gathering data and sorting it, to compile a host of cyberpunk-information related documents and work. The TCP started in 1996 and was actively supported until late 2002."

11. Levy, *Hackers*, 451.

12. Levy, *Hackers*, 169–170.

13. Levy, *Hackers*, 164–165.

14. Levy, *Hackers*, 222.

15. Levy, *Hackers*, 276, 458–459.

16. Levy, *Hackers*, 437–450; Richard Stallman, correspondence with the author, December 17, 2017.

17. Levy, *Hackers*, 448.

18. Levy, *Hackers*, 450. In his book, Levy divides hackers by generation into "true hackers" (the MIT hackers), "microcomputer hackers" and "game hackers". So the statement he assigns to Stallman means that Stallman believed he was the last of his generation of hackers at MIT, not that no other hackers existed at the time.

19. Levy, *Hackers*, 447, 450.

20. Attributed to the early Jewish leader Hillel.

21. Initially, Stallman stipulated only the last, three freedoms, and numbered them 1 to 3. Then he realized it was necessary to articulate a fourth freedom, which he wanted to state first, so he numbered it 0, which was apt because computers count from 0 and not 1. Author's communication with Richard Stallman, March 4, 2019.

22. Richard Stallman, "The Initial Announcement of the GNU Operating System," in *Free Software, Free Society: Selected Essays of Richard M. Stallman* (Boston: Free Software Foundation, 2002), 26–27. It is interesting that in his initial announcement Stallman said he planned to give his software away for free, however, it is important to remember that "gratis" or "given away at no cost" is *not* part of the definition of free software.

23. Richard Stallman, "Releasing Free Software If You Work at a University," in *Free Software, Free Society*, 63.

24. Gerard Alberto and Ruth Oldenzeil, eds., *Hacking Europe: From Computer Cultures to Demoscenses* (London: Springer-Verlag, 2014), 8–9.

25. Alberto and Oldenzeil, *Hacking Europe*, 17.

26. Kai Denker, "Heroes Yet Criminals of the German Computer Revolution," in Alberto and Oldenzeil, *Hacking Europe*, 171, citing a biography on the Chaos Computer Club's cofounder Wau Holland written by Daniel Kulla, *Der Phrasenprüfer. Szenen aus dem Leben von Wau Holland* (Löhrbach: Pieper and the Grüne Kraft, 2003),16.

27. Denker, "Heroes Yet Criminals," 171, citing Kulla, *Der Phrasenprüfer*, 20.

28. Denker, "Heroes Yet Criminals," 170.

29. Denker, "Heroes Yet Criminals," 172.

30. Denker, "Heroes Yet Criminals," 168.

31. Caroline Nevejan and Alexander Badenoch, "How Amsterdam Invented the Internet: European Networks of Significance, 1980–1995," in Alberto and Oldenzeil, *Hacking Europe*, 199.

32. For extended details about this KGB hack story, see the collection of contemporary news articles in *Phrack World News*, part 2, no. 25 (March 29, 1989), http://phrack.org/issues/25/10.html.

33. Reenactment of the Wau-Pengo debate (1989) at the 31st Congress of the Chaos Computer Club (31C3), Wau Holland Foundation, https://www.wauland.de/en/index.php. The reenactors in this video use a transcript. I transcribed the interview from this video to make my own transcript and have used excerpts from the transcript without showing the gaps to make reading the conversation easier. The excerpts are in the order they were spoken.

34. The early Dutch entrepreneur and tech journalist Luc Sala described the after party and the kind of cross-fertilization that was going on between the European and California scenes around this time in a "personal perspective" on the early hacker/New Age magazine *Mondo 2000*. He stayed for some time in the communal Mondo house in Berkeley and ended up driving across the country in winter with John Perry Barlow to the latter's ranch in Wyoming. He wrote about the California scene in "New Age & Mondo: A Personal Perspective—Part 1," Mondo 2000 History Project Entry #8, Acceler8or, March 28, 2012, https://www.acceler8or.com/tags/chaos-computer-club:

> Psychedelics were the not so secret but illicit link between the various subworlds of art, literature, music, new age and technology. … convergence … was the hallmark of Mondo. They covered the whole gamut of alternativity. …
>
> As this was the Bay Area and Silicon Valley was close, the link with the computer industry was easy and logical. There was the money and the excitement. In those days everybody looked at the new possibilities, whether it was in music with synthesizers; in broadcasting with digital media; in entertainment with the emerging computer games. And virtual reality was definitely the magic potion that would free us from the limitations of space and time, the ultimate trip, the electronic drug. Most of the people involved had a sixties background, although there were also the catch-up hippies like myself, who missed out on but were fascinated by the likes of Leary and the Zeitgeist of the sixties.

35. Re-enactment of the Wau-Pengo debate.

36. In German, an *eingetragener verein*.

37. Katie Krause and Ole Schultz, "Our Own Private Germany," *Matter*, November 7, 2014, https://medium.com/matter/our-own-private-germany-6ce44ac93a7b.

38. Krause and Schultz, "Our Own Private Germany."

39. Gerard Alberto and Ruth Oldenziel, "Introduction: How European Players Captured the Computer and Created Scenes," in Alberto and Oldenzeil, *Hacking Europe*, 1–2.

40. Academics have done a lot of work pointing this out. See the important work of Gabriella Coleman, Alex Golub, Chris Kelty, and Molly Sauter on this subject. Journalist Bruce Sterling has also acknowledged the story is more complicated than Levy has told it. Although I have distinguished the cultural origins of hacking in different European countries, there is not space in this book to cover in any detail other groups like the early phone phreakers or the hacker underground (Julian Assange's habitat as a young hacker) that emerged out of the phreakers, except briefly where the latter intersects with Assange's story. Nor do I cover in detail some of the early groups that used distributed denial of service (DDoS) tactics for political protest, although I do mention some of these in chapter 11.

41. Read the Wau-Pengo debate transcribed at some length in this chapter. Wau Holland cites the hacker ethic as Levy summarized it.

42. As is mentioned in chapters 2 and 11, both Assange and Anonymous have explicitly espoused free software principles at various times.

43. Stallman received the award in 1990. The World Wide Web was invented in 1991.

44. Levy, *Hackers: Heroes of the Computer Revolution*, 271.

45. It is estimated that contributors to Torvalds's Linux project number in the hundreds of thousands and that its code is now more than 19 million lines long. Craig Timberg, "Net of Insecurity: The Kernel of the Argument," *Washington Post*, November 3, 2015.

46. Stallman, "Releasing Free Software If You Work at a University," 64–66.

47. Timberg, "Net of Insecurity."

48. Sebastian Anthony, "International Space Station Switches from Windows to Linux, for Improved Reliability," *Extreme Tech*, May 9, 2013, https://www.extremetech.com/extreme/155392-international-space-station-switches-from-windows-to-linux-for-improved-reliability.

49. Aaron Pressman, "The iPhone Decade: One of the Tech Industry's Biggest Innovations Celebrates Its Tenth Anniversary," *Fortune*, June 1, 2015, 25.

50. Timberg, "Net of Insecurity." According to Richard Stallman, GNU/Linux is used in internet servers, the New York stock exchange, the platforms of Google, Facebook and Amazon, and in many other places. Author's correspondence with Richard Stallman, March 4, 2019.

51. Richard Stallman, correspondence with the author, September 17, 2018. See also https://www.gnu.org/philosophy/open-source-misses-the-point.en.html.

52. Author's communication with Richard Stallman, March 4, 2019.

53. Unless a new free software smart phone comes onto the market in the meantime. One currently in development by Purism is the Librem phone. It is made entirely with free software, including its kernel. Richard Stallman, communication with author, July 6, 2019.

54. Pressman, "The iPhone Decade."

55. Leon Trotsky, *My Life: An Attempt at an Autobiography* (New York: Dover, 2017), 215.

56. General Keith Alexander was the director of the US National Security Agency from 2005 to 2013. He famously advocated that security agencies should "collect the whole haystack" of personal digital information available, rather than bothering with legal warrants to look for "needles" or specific information.

57. "The 2600 crowd" refers to the name of a publication, *2600: The Hacker Quarterly*, and an associated conference that grew out of a culture of early telephone hackers in the United States known as *phreakers*. In the 1960s, these early hackers discovered that a 2600 hertz tone (which could be reproduced with a toy whistle from a Cap'n Crunch cereal box), would allow them "operator" access to phone systems. "*2600: The Hacker Quarterly*," Wikipedia, https://en.wikipedia.org/wiki/2600:_The_Hacker_Quarterly (accessed January 1, 2019).

58. Although he has never openly admitted it, Assange has hinted that he was responsible for the notorious WANK worm attack on NASA, too. See Robert Manne, "The Cypherpunk Revolutionary," *The Monthly*, March 2011, https://www.themonthly.com.au/issue/2011/february/1324596189/robert-manne/cypherpunk-revolutionary: "By October 1989 an attack was mounted from Australia on the NASA computer system via the introduction of what was called the WANK worm in

an attempt to sabotage the Jupiter launch of the *Galileo* rocket as part of an action of anti-nuclear activists. No one claimed responsibility for this attack, which is outlined in the first chapter of *Underground*. In an article he later published in the left-wing magazine *CounterPunch*, Assange would claim the WANK worm attack was 'the origin of hacktivism.' In a Swedish television documentary, *WikiRebels*, made with Assange's co-operation, there are hints he was responsible."

59. Manne, "The Cypherpunk Revolutionary."

60. Andrew Greenberg, *This Machine Kills Secrets: Julian Assange, the Cypherpunks, and Their Fight to Empower Whistleblowers* (New York: Plume, 2012), 96.

61. And the start of a brave new world. Aldous Huxley's 1932 novel, *Brave New World*, about a technological dystopia, takes its title from Miranda's speech in William Shakespeare's play, *The Tempest* (act 5, scene 1): "Oh, wonder! / How many goodly creatures are there here! / How beauteous mankind is! O brave new world, / That has such people in't."

CHAPTER 2

1. The "Collateral Murder" video was leaked by Bradley Manning to WikiLeaks. Taken from a US military helicopter, it shows gunsight footage of Iraqi civilians being killed. Crew members can be heard chatting as if they are playing a game. Assange decided that this was the leak to edit and package for the press, and it made WikiLeaks a household name.

2. Bruce Sterling, "The Blast Shack," *Webstock*, December 22, 2010, http://www.webstock.org.nz/the-blast-shack. In fact, Sterling thought the cablegate affair was a "dismal saga" and a "melancholy business": "it's going to take me a while to explain why this highly newsworthy event fills me with such a chilly, deadening sense of Edgar Allan Poe melancholia. But it sure does. Part of this dull, icy feeling, I think, must be the agonizing slowness with which this has happened. At last—at long last—the homemade nitroglycerin in the old cypherpunks blast shack has gone off."

3. Andrew Greenberg, *This Machine Kills Secrets: Julian Assange, the Cypherpunks, and Their Fight to Empower Whistleblowers* (New York: Plume, 2012), 58.

4. See "Cypherpunk," Activism.net, https://activsm.net/cypherpunk/crypto-anarchy.html (accessed June 20, 2018).

5. Greenberg, *This Machine Kills Secrets*, 52.

6. Greenberg, *This Machine Kills Secrets*, 78–79.

7. Timothy C. May, "The Cyphernomicon," version 0.666, September 10, 1994, http://www.kreps.org/hackers/overheads/11cyphernervs.pdf.

8. Greenberg, *This Machine Kills Secrets,* 81.

9. May, "The Cyphernomicon."

10. May, "The Cyphernomicon."

11. Robert Manne, "The Cypherpunk Revolutionary," *The Monthly*, March 2011, https://www.themonthly.com.au/issue/2011/february/1324596189/robert-manne/cypherpunk-revolutionary.

12. May, "The Cyphernomicon."

13. May, "The Cyphernomicon."

14. May, "The Cyphernomicon."

15. Eric Hughes, "A Cypherpunk's Manfesto," 1993, https://www.digitalmanifesto.net/manifestos/16.