INTRODUCTION

In the fall of 2005, without much in the way of grandiose expectations, I decided to create a political blog. I had little idea at the time how much this decision would eventually change my life. My principal motive was that I was becoming increasingly alarmed by the radical and extremist theories of power the US government had adopted in the wake of 9/11, and I hoped that writing about such issues might allow me to make a broader impact than I could in my then-career as a constitutional and civil rights lawyer.

Just seven weeks after I began blogging, the *New York Times* dropped a bombshell: in 2001, it reported, the Bush administration had secretly ordered the National Security Agency (NSA) to eavesdrop on the electronic communications of Americans without obtaining the warrants required by relevant criminal law. At the time that it was revealed, this warrantless eavesdropping had been going on for four years and had targeted at least several thousand Americans.

The subject was a perfect convergence of my passions and my expertise. The government tried to justify the secret NSA program by invoking exactly the kind of extreme theory of executive power that had motivated me to begin writing: the notion that the threat of terrorism vested the president with virtually unlimited authority to do anything to "keep the

nation safe," including the authority to break the law. The ensuing debate entailed complex questions of constitutional law and statutory interpretation, which my legal background rendered me well suited to address.

I spent the next two years covering every aspect of the NSA warrantless wiretapping scandal, on my blog and in a bestselling 2006 book. My position was straightforward: by ordering illegal eavesdropping, the president had committed crimes and should be held accountable for them. In America's increasingly jingoistic and oppressive political climate, this proved to be an intensely controversial stance.

It was this background that prompted Edward Snowden, several years later, to choose me as his first contact person for revealing NSA wrongdoing on an even more massive scale. He said he believed I could be counted on to understand the dangers of mass surveillance and extreme state secrecy, and not to back down in the face of pressure from the government and its many allies in the media and elsewhere.

The remarkable volume of top secret documents that Snowden passed on to me, along with the high drama surrounding Snowden himself, have generated unprecedented worldwide interest in the menace of mass electronic surveillance and the value of privacy in the digital age. But the underlying problems have been festering for years, largely in the dark.

There are, to be sure, many unique aspects to the current NSA controversy. Technology has now enabled a type of ubiquitous surveillance that had previously been the province of only the most imaginative science fiction writers. Moreover, the post-9/11 American veneration of security above all else has created a climate particularly conducive to abuses of power. And thanks to Snowden's bravery and the relative ease of copying digital information, we have an unparalleled firsthand look at the details of how the surveillance system actually operates.

Still, in many respects the issues raised by the NSA story resonate with numerous episodes from the past, stretching back across the centuries. Indeed, opposition to government invasion of privacy was a major factor in the establishment of the United States itself, as American colonists protested laws that let British officials ransack at will any home they wished. It was legitimate, the colonists agreed, for the state to obtain specific, targeted warrants to search individuals when there was evidence

to establish probable cause of their wrongdoing. But general warrants—the practice of making the entire citizenry subject to indiscriminate searches—were inherently illegitimate.

The Fourth Amendment enshrined this idea in American law. Its language is clear and succinct: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." It was intended, above all, to abolish forever in America the power of the government to subject its citizens to generalized, suspicionless surveillance.

The clash over surveillance in the eighteenth century focused on house searches, but as technology evolved, surveillance evolved with it. In the mid-nineteenth century, as the spread of railways began to allow for cheap and rapid mail delivery, the British government's surreptitious opening of mail caused a major scandal in the UK. By the early decades of the twentieth century, the US Bureau of Investigation—the precursor of today's FBI—was using wiretaps, along with mail monitoring and informants, to clamp down on those opposed to American government policies.

No matter the specific techniques involved, historically mass surveillance has had several constant attributes. Initially, it is always the country's dissidents and marginalized who bear the brunt of the surveillance, leading those who support the government or are merely apathetic to mistakenly believe they are immune. And history shows that the mere existence of a mass surveillance apparatus, regardless of how it is used, is in itself sufficient to stifle dissent. A citizenry that is aware of always being watched quickly becomes a compliant and fearful one.

Frank Church's mid-1970s investigation into the FBI's spying shockingly found that the agency had labeled half a million US citizens as potential "subversives," routinely spying on people based purely on their political beliefs. (The FBI's list of targets ranged from Martin Luther King to John Lennon, from the women's liberation movement to the anti-Communist John Birch Society.) But the plague of surveillance abuse is

hardly unique to American history. On the contrary, mass surveillance is a universal temptation for any unscrupulous power. And in every instance, the motive is the same: suppressing dissent and mandating compliance.

Surveillance thus unites governments of otherwise remarkably divergent political creeds. At the turn of the twentieth century, the British and French empires both created specialized monitoring departments to deal with the threat of anticolonialist movements. After World War II, the East German Ministry of State Security, popularly known as the Stasi, became synonymous with government intrusion into personal lives. And more recently, as popular protests during the Arab Spring challenged dictators' grasp on power, the regimes in Syria, Egypt, and Libya all sought to spy on the Internet use of domestic dissenters.

Investigations by Bloomberg News and the *Wall Street Journal* have shown that as these dictatorships were overwhelmed by protestors, they literally went shopping for surveillance tools from Western technology companies. Syria's Assad regime flew in employees from the Italian surveillance company Area SpA, who were told that the Syrians "urgently needed to track people." In Egypt, Mubarak's secret police bought tools to penetrate Skype encryption and eavesdrop on activists' calls. And in Libya, the *Journal* reported, journalists and rebels who entered a government monitoring center in 2011 found "a wall of black refrigerator-size devices" from the French surveillance company Amesys. The equipment "inspected the Internet traffic" of Libya's main Internet service provider, "opening emails, divining passwords, snooping on online chats and mapping connections among various suspects."

The ability to eavesdrop on people's communications vests immense power in those who do it. And unless such power is held in check by rigorous oversight and accountability, it is almost certain to be abused. Expecting the US government to operate a massive surveillance machine in complete secrecy without falling prey to its temptations runs counter to every historical example and all available evidence about human nature.

Indeed, even before Snowden's revelations, it was already becoming clear that treating the United States as somehow exceptional on the issue

of surveillance is a highly naive stance. In 2006, at a congressional hearing titled "The Internet in China: A Tool for Freedom or Suppression?," speakers lined up to condemn American technology companies for helping China suppress dissent on the Internet. Christopher Smith (R-NJ), the congressman presiding over the hearing, likened Yahoo!'s cooperation with Chinese secret police to handing Anne Frank over to the Nazis. It was a full-throated harangue, a typical performance when American officials speak about a regime not aligned with the United States.

But even the congressional attendees couldn't help noting that the hearing happened to take place just two months after the *New York Times* revealed the vast warrantless domestic wiretapping carried out by the Bush administration. In light of those revelations, denouncing other countries for carrying out their own domestic surveillance rang rather hollow. Representative Brad Sherman (D-CA), speaking after Representative Smith, noted that the technology companies being told to resist the Chinese regime should also be careful regarding their own government. "Otherwise," he warned prophetically, "while those in China may see their privacy violated in the most heinous ways, we here in the United States may also find that perhaps some future president asserting these very broad interpretations of the Constitution is reading our e-mail, and I would prefer that not happen without a court order."

Over the past decades, the fear of terrorism—stoked by consistent exaggerations of the actual threat—has been exploited by US leaders to justify a wide array of extremist policies. It has led to wars of aggression, a worldwide torture regime, and the detention (and even assassination) of both foreign nationals and American citizens without any charges. But the ubiquitous, secretive system of suspicionless surveillance that it has spawned may very well turn out to be its most enduring legacy. This is so because, despite all the historical parallels, there is also a genuinely new dimension to the current NSA surveillance scandal: the role now played by the Internet in daily life.

Especially for the younger generation, the Internet is not some standalone, separate domain where a few of life's functions are carried out. It is not merely our post office and our telephone. Rather, it is the epicenter

of our world, the place where virtually everything is done. It is where friends are made, where books and films are chosen, where political activism is organized, where the most private data is created and stored. It is where we develop and express our very personality and sense of self.

To turn *that* network into a system of mass surveillance has implications unlike those of any previous state surveillance programs. All the prior spying systems were by necessity more limited and capable of being evaded. To permit surveillance to take root on the Internet would mean subjecting virtually all forms of human interaction, planning, and even thought itself to comprehensive state examination.

From the time that it first began to be widely used, the Internet has been seen by many as possessing an extraordinary potential: the ability to liberate hundreds of millions of people by democratizing political discourse and leveling the playing field between the powerful and the powerless. Internet freedom—the ability to use the network without institutional constraints, social or state control, and pervasive fear—is central to the fulfillment of that promise. Converting the Internet into a system of surveillance thus guts it of its core potential. Worse, it turns the Internet into a tool of repression, threatening to produce the most extreme and oppressive weapon of state intrusion human history has ever seen.

That's what makes Snowden's revelations so stunning and so vitally important. By daring to expose the NSA's astonishing surveillance capabilities and its even more astounding ambitions, he has made it clear, with these disclosures, that we stand at a historic crossroads. Will the digital age usher in the individual liberation and political freedoms that the Internet is uniquely capable of unleashing? Or will it bring about a system of omnipresent monitoring and control, beyond the dreams of even the greatest tyrants of the past? Right now, either path is possible. Our actions will determine where we end up.

1

CONTACT

On December 1, 2012, I received my first communication from Edward Snowden, although I had no idea at the time that it was from him.

The contact came in the form of an email from someone calling himself Cincinnatus, a reference to Lucius Quinctius Cincinnatus, the Roman farmer who, in the fifth century BC, was appointed dictator of Rome to defend the city against attack. He is most remembered for what he did after vanquishing Rome's enemies: he immediately and voluntarily gave up political power and returned to farming life. Hailed as a "model of civic virtue," Cincinnatus has become a symbol of the use of political power in the public interest and the worth of limiting or even relinquishing individual power for the greater good.

The email began: "The security of people's communications is very important to me," and its stated purpose was to urge me to begin using PGP encryption so that "Cincinnatus" could communicate things in which, he said, he was certain I would be interested. Invented in 1991, PGP stands for "pretty good privacy." It has been developed into a sophisticated tool to shield email and other forms of online communications from surveillance and hacking.

The program essentially wraps every email in a protective shield, which is a code composed of hundreds, or even thousands, of random