The End of Social Media Revolutions

Sarah Lange

On July 7, 2011, a series of violent explosions rocked the small town of Abadan, Turkmenistan, located only a short distance from the capital city of Ashgabat. The explosions sent massive plumes of black smoke and flames into the air, shattering windows, destroying schools and apartment buildings, and killing an unknown number of citizens.[1] It was later discovered that a munitions depot in the small city had caught fire, the cause of which remains unclear.[2] In the immediate aftermath of the explosions, cellphone communication in the city was cut off. The state television channel aired only Turkmen musical programs and offered no information on the event or instructions for relatives to contact family members in the area.[3] There were also reports of the Internet itself being shutdown throughout the entire country.[4] An official statement from the Government of Turkmenistan the following day reported, "There are no victims or particular wreckages. The population is being provided the necessary medical and other forms of assistance. Some of the population which lives immediately adjacent to the location of the incident ha[s] been evacuated to a safe place."[5] In contrast to these statements, an alternative news website for the country, Chrono-TM.org,[6] reported the death toll to be around 200 people,[7] that apartment buildings had been destroyed, and that a local school had caught fire.

Sarah Lange *is the Executive Director of the Arzuw Foundation, a non-profit organization dedicated to supporting the next generation of leaders in Turkmenistan. Sarah has been working and conducting research in Central Asia since 2006 and was awarded a Fulbright Fellowship to Kazakhstan in 2007. She holds a B.A. from Tufts University in International Relations and Russian language and has just completed her M.A. from the Fletcher School through the Global Master of Arts Program. The opinions in this piece are those of Sarah Lange and not of the Arzuw Foundation.*

Within twenty-four hours of the explosions, the government's official position on the events was delegitimized by reports from citizen journalists who used cellphones to record the explosions and wreckage, and communicated eyewitness reports to watchers of Turkmenistan abroad. Although it took several days before the government admitted any human loss, it eventually reported fifteen total casualties, including two soldiers.[8]

This offered Turkmenistan's citizens an unprecedented experience of the potential modern information and communication technologies (ICTs) possess to shift the balance of power from sovereign to citizen.

The "change-of-story" itself was quite remarkable in this notoriously hermetic country, which is tied with North Korea for the world's most repressive press environment in Freedom House's 2013 Freedom of the Press Rankings.[9] While still incongruous with eyewitness reports, the authorities in Turkmenistan were not able to maintain their sanitized version of the truth. This offered Turkmenistan's citizens an unprecedented experience of the potential modern information and communication technologies (ICTs) possess to shift the balance of power from sovereign to citizen in even the most repressive authoritarian regimes.

Following the 2004 Orange Revolution in Ukraine, Iran's Green Movement in 2009, and later during the popular uprisings of the Arab Spring, academics, journalists and bloggers produced a great deal of speculation and analysis about the potential of ICTs to empower civil society in challenging authoritarian regimes around the world through non-violent civil resistance. In his 2009 book, *Here Comes Everybody,* Clay Shirky extolled the ability of the Internet to fundamentally change the way social activism takes place, as new communication tools are now flexible enough to "match our social capabilities"[10] and thus provide opportunities for new types of social activism to occur. On the other hand, writing in the *New Yorker* in 2010, Malcolm Gladwell questioned the power of ICTs to transform activism, arguing that "high-risk," "strategic" activism like that witnessed during the American Civil Rights movement in the 1960s may be assisted—but not transformed—by ICTs.[11] The world of ICTs that Shirky and Gladwell analyzed only a few years ago has since changed significantly, rendering this debate now obsolete. While Western democracy advocates debated the potential of "liberation technologies"[12] to empower repressed populations to challenge authoritarianism, repressive regimes were quietly but actively acquiring Western-produced mass surveillance technologies that completely and utterly obliterate the liberating potential of ICTs.

THE CONFLUENCE OF MODERN COMMUNICATION AND CIVIL RESISTANCE

The emergence of the wired communication era, marked by the advent of the telegraph in 1844, coincided with the beginning of a historical shift in the power dynamic between citizens and their sovereigns around the world. In 1867, a campaign of "legal resistance" seeking more autonomy and national rights by Hungarians living under the Hapsburg monarchy was one of the first non-violent civil resistance movements that achieved a degree of success.[13] During this period, and the decades that followed, a confluence of geopolitics, world wars, and technological innovation changed the power dynamic between citizen and state. This also created new opportunities for repressive regimes to be held accountable by their citizens through non-violent conflict. The evolution of this power dynamic continued to progress from the mid-1800s onward, with the defining event arguably being the powerful civil resistance movement against the British in India led by Mohandas Gandhi in 1930-1931.[14] From that point forward it is possible to observe the interplay between the use of new communication tools to liberate and empower civil society, and the response of governments to control that communication. This relationship had been steadily and consistently evolving since the first telegraph was sent across the wires on May 24, 1844 with the ominous message, "What hath God Wrought?"[15]

During this period, and the decades that followed, a confluence of geopolitics, world wars, and technological innovation changed the power dynamic between citizen and state.

Communication has been a critical and essential component of the organization and mobilization of popular protest movements throughout the twentieth century and into the twenty-first century, and it is therefore the disruption and control of communication that has become the target of repressive governments seeking to limit the power of their people. In response to today's rapidly expanding adoption of communication tools such as social media and smartphones, a new generation of highly sophisticated mass surveillance technologies has emerged that allows states to control and monitor these modern communications with unprecedented accuracy, thoroughness, and ease. Developed in Western democracies and purchased by countries like Libya, Syria, Egypt, and Bahrain, mass surveillance technologies allow effortless, real-time tracking and monitoring of any citizen using any communication method that connects to the Internet or a

cellular network. Mass surveillance technologies like FinSpy and Blue Coat alter the balance of power between citizen and sovereign in authoritarian regimes by overwhelmingly shifting the power balance to the advantage of repressive regimes. This surveillance is not only taking place inside authoritarian regimes, but is also employed by these regimes against targets in democratic countries, including the United States and the United Kingdom,[16] empowering repressive regimes to control and monitor activist networks inside their own borders and beyond.

Mass surveillance technologies like FinSpy and Blue Coat alter the balance of power between citizen and sovereign in authoritarian regimes by overwhelmingly shifting the power balance to the advantage of repressive regimes.

In June 2013, articles in *The Guardian* and the *Washington Post* confirmed the existence of powerful mass surveillance programs in both Britain and the United States[17] revealing how intense the struggle to control communication is between citizen and sovereign in even the world's most established democracies. As Western produced mass surveillance tools further empower repressive regimes around the world, citizens of the democratic West must now also decide what role mass surveillance has in a democracy. The balance of power within a democracy is not static, but rather constantly shifts between citizen and state. It is this continuous movement of the balance of power that ensures the health and perpetuation of democracy. The preeminent difference between mass surveillance programs in democracies like the United States and those employed by authoritarian regimes is the existence of constitutional controls and judicial oversight that can be exercised to review such programs and reign in the extent of their reach. In authoritarian regimes no such control mechanism exists leaving the state with an unfettered ability to completely and absolutely monitor its citizens with terrifying accuracy and ease.

The mass surveillance industry is highly secretive, making it difficult to know just how quickly it is growing; however, there is evidence to suggest that demand for these products is on the rise. When CitizenLab researchers were first able to acquire and analyze copies of a software used by the Bahraini authorities[18] to monitor civil society activists after the events of the Arab Spring in July 2012, they released a report citing evidence of "one of the world's best-known and elusive cyber weapons: FinFisher … which can secretly take remote control of a computer, copying files,

intercepting Skype calls and logging every keystroke."[19] In the spring of 2013, CitizenLab detected a total of thirty-six FinSpy servers[20] around the world, seven of which were in countries that had not shown up in the previous year's scan.[21] Mass surveillance technologies produced by Western countries including the United States, United Kingdom, Finland, Sweden, Denmark, Ireland, Germany, Italy, and France have shown up in some of the most repressive corners of the world, including Turkmenistan, Sudan, Libya, Syria, Tunisia, Bahrain, Iran, and Vietnam.

NO TRUST, NO PRIVACY, NO DEMOCRACY

Mass surveillance technologies work to not only control and destroy the liberating potential of ICTs, they also work on a deeper and more insidious level, just as all state surveillance does in states without adequate judicial and constitutional controls, or when such programs operate secretly and unchecked by the populace in even established democracies. These technologies have the ability to undermine the liberating power of ICTs, and to inhibit civil society from mounting a disciplined and coordinated non-violent civil resistance campaign to claim the power balance in an authoritarian state or to check the power of the government in a democracy. Furthermore, they weaken civil society itself by undermining the existence of privacy and trust within a state. The resulting effect is that in the absence of trust and privacy, the ability of civil society to balance the power of the state is diminished, and the state, whether democratic or authoritarian, is permitted a greater retention of power.

The degrees to which privacy and trust exist within a country are the primary determinants of the balance of power between citizen and state. Privacy itself is an elusive concept to define. The idea of privacy is complex and understandings of privacy are deeply dependent on cultural norms and shared values.[22] Even within a society with a shared historical experience, privacy is an emotionally charged and even divisive issue of debate; it is a debate whose resolution is evasive largely because "[n]o single meme or formulation of privacy's purpose has emerged around which privacy advocacy might coalesce."[23] Dourish and Anderson define privacy not as what it *is* but rather what it *does*.[24] They describe privacy as a social consideration, to which the risks of solitude, autonomy, and confidentiality are primary concerns.[25] Privacy is vital for the establishment and maintenance of the associations and group identities that help to create civil society. Julie Cohen describes privacy in this way: "privacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to

render individuals and communities fixed, transparent, and predictable. It protects the situated practices of boundary management through which the capacity for self-determination develops."[26] Dourish and Anderson concur with Cohen's assessment of the role privacy plays in "boundary management." They describe the intertwining relationship between secrecy, trust, and identity in which secrets are used in social boundary management and it is the keeping and managing of those secrets that "are ways in which affiliation and membership are managed and demonstrated."[27] It is the private sharing of this information that works to create and solidify bonds between those who have the information and those who do not,[28] and thus serves an essential function in civil society.

Privacy and democracy are best understood not as separate concepts or as concepts developing separately from one another; they are intrinsically linked.[29] It is an unwritten contract between citizens and their sovereign in democratic countries that no individual is allowed absolute privacy—all citizens must sacrifice a degree of privacy for the sake of security. Under certain conditions a democracy may also limit the privacy of its citizens, especially in times of war or in cases of libel or defamation.[30] The relationship between security and privacy is a pendulum that swings in a democracy; a perfect balance is never achieved, but it is one that is constantly being evaluated and negotiated between the citizen and the state. What distinguishes privacy under a democracy from that in an authoritarian regime is that this pendulum does swing relatively freely and that "surveillance is seen as the exception, not the rule."[31] Under an authoritarian regime, it is rarely, if ever, the case that once privacy is surrendered to the state, it is ever returned to the people by that regime. This loss of privacy translates into a gain in absolute power by the state. Extrapolating from this causation, it can be said that in a democracy or in an authoritarian state in which there are no limits to, or oversight of surveillance, the health of or emergence of democracy will be threatened or inhibited by the absence of privacy.

The relationship between security and privacy is a pendulum that swings in a democracy; a perfect balance is never achieved, but it is one that is constantly being evaluated and negotiated between the citizen and the state.

Trust, like privacy, is itself inherent in the relationship between a citizen and a democratic government. John Locke described this trust-based existence by stating that, "the liberty of man, in society, is to be

under no other legislative power, but that established, by consent, in the common-wealth; nor under the dominion of any will, or restraint of any law, but what that legislative shall enact, according to the trust put in it."[32] Trust must exist for individuals to participate voluntarily in the political, social and economic institutions of a state and is required for the establishment of civil society;[33] it is what allows citizens, who in a liberal democracy exercise control over their government through representative institutions, to rely on the democratic process even if they have short term grievances with their elected government.[34] It is the trust of civil society in the system itself that allows democracy to be perpetuated to the next election.

Robert Putnam, in his seminal work on civil society in Italy, described the important role of trust in civil society. In the "civic community," where honesty, trust and law-abidingness exist, citizens "deal fairly with one another and expect fair dealings in return."[35] Citizens of these communities hold their government to high standards and so long as those standards are met, they themselves are willing to follow high standards. Putnam observes that it is also the case in a community without these virtues, or less of them, that "life is riskier, citizens are warier, and the laws, made by higher-ups are made to be broken."[36] Observing the impact of a lack of trust in a society, Putnam states, "societies which rely heavily on the use of force are likely to be less efficient, more costly, and more unpleasant than those where trust is maintained by other means."[37]

Kenneth Newton differentiates between social and political trust. He observes, "political trust and social trust are similar in some ways but different in others. Social … trust can be based upon immediate, first hand experience of others, whereas political trust is most generally learned indirectly and at a distance, usually through the media."[38] Newton argues that an analysis of trust should not focus on an individual's level of trust but rather on the "trustworthiness of society at large."[39] However, these two types of trust are not entirely independent of one another: a relationship does exist if not at the individual level than at the systemic level.[40] Newton takes the ideas advanced by Putnam and integrates these concepts into a systemic-level explanation of trust, asserting that because civil society is a "collective property of social systems" rather than an individual characteristic, the "relationship is found at the aggregate level of society as a whole."[41] He concludes, "countries with relatively high levels of social trust tend to have relatively high levels of political confidence as well."[42] Trust is also something that may at first be inherited by way of historical legacy, but over the long-term, is itself earned based on the performance of the government,[43] which contributes to a healthy balance of power between citizen

and state in democratic countries. In the absence of trust there is only distrust, which weakens civil society and allows the state to enjoy a greater concentration of power. Fukuyama describes the process through which horizontal trust in Bolshevik Russia was broken by a centralizing state seeking to destroy the trust within civil society in favor of vertical-only associations with the state. [44] He described the result as a "post-Soviet society bereft of both trust and a durable civil society."[45] When governments secretly and indiscriminately monitor private communication without the consent of their people, evidence from which may be used to arrest or even torture individuals, the trust between citizen and state is eroded and the result is a weakened, distrustful civil society.

When governments secretly and indiscriminately monitor private communication without the consent of their people, evidence from which may be used to arrest or even torture individuals, the trust between citizen and state is eroded and the result is a weakened, distrustful civil society.

Thomas Schelling wrote of the power balance between authoritarian regimes and their citizens,

> The tyrant and his subjects are in somewhat symmetrical positions. *They* can deny *him* most of what *he* wants – they can, that is, if they have the disciplined organization to refuse collaboration. And *he* can deny *them* just about everything they want … It is a bargaining situation in which either side, if adequately disciplined and organized, can deny most of what the other wants, and it remains to see who wins.[46]

It is possible for civil society to succeed in shifting the power balance within even brutal, authoritarian regimes in their favor through non-violent conflict. But this strategy requires unity, concerted planning, and non-violent discipline.[47] Such a strategy demands the existence of trust within civil society, the ability of citizens to communicate privately, and the social cohesion to unify around a single goal. Without trust, without privacy, and without the ability to communicate securely, a population is severely crippled in its ability to achieve this level of organization.

Ukraine's 2004 Orange Revolution

The 2004 Orange Revolution in Ukraine was the first large-scale, non-violent conflict that utilized the Internet and cellphones to organize

and rally supporters to protest the results of its presidential election.[48] The Internet played an important role in these demonstrations as it "leveled the playing field in the Ukrainian election by successfully disseminating information through non-traditional channels."[49] During the events of the Orange Revolution, when television was heavily censored, "the Internet was the only medium through which one could find answers to basic questions: What is the date and location of the next meeting? What are the plans of the opposition? What is happening on the street? Sometimes events unfolded so rapidly that only Internet media provided people with up-to-date information."[50] An analysis of the events in 2004 concluded, "in the case of Ukraine it is evident that pro-democracy forces used the Internet and cellphones more effectively than the pro-government forces, such that in this specific time and place these technologies weighed in on the side of democracy."[51]

The protestors in 2004 were, in many respects, fortunate that events prior to the protests created an environment in which these technologies gave them, and not the government, the advantage. In the years prior to the protest, Internet penetration in Ukraine was quite low and usage was only around 3-4 percent of the population.[52] During 2002, the Social Democratic Party of Ukraine invested a significant amount of time and money in an Internet campaign, but by 2004 it had "lost interest in the Internet"[53] after the efforts produced disappointing results. The opposition party led by Viktor Yushchenko, however, made more active use of the Internet as a communication tool and thus was arguably more prepared to take advantage of the Internet as a protest tool in 2004.

When the Internet age arrived in Ukraine, and coincided with a popular protest, the government was simply unprepared to control its power. As the events of the Orange Revolution unfolded, protestors utilized the Internet to their own ends. As political tension intensified after the elections, more and more users were drawn to the Internet. For instance, the news site *Ukrainska Pravda* drew 800,000 hits in the first round of elections and 1,800,000 hits during the third round of elections.[54] The government made attempts in the months immediately prior to the revolution to censor some anti-government jokes and material online, but the Internet remained largely unregulated throughout the

In Ukraine in 2004, civil society had the technological edge in communications and it succeeded in securing a revote in their presidential election.

protests.[55] In Ukraine in 2004, civil society had the technological edge in communications and it succeeded in securing a revote in their presidential election.

As proponents of democracy around the world were watching and cheering on the waves of orange in Ukraine's Independence Square, particularly astute authoritarian regimes such as that in Iran were also watching with great interest. The Orange Revolution left many around the world, particularly in the West, optimistic about the potential of ICTs to empower civil society to challenge authoritarianism, but the same events also inspired repressive regimes to devise new strategies to control and monitor ICTs that could be used to organize popular protests by their own citizens. The Iranian regime has perhaps been one of the most efficient regimes in this learning process and has, as a result, proved extremely proficient at preparing for and anticipating the next popular protest—as was evident in 2009.

Iran's 2009 Green Movement

After the success of the Orange Revolution, it was not until June 2009 that the world again had an opportunity to witness the potential of ICTs to facilitate non-violent civil resistance movements opposing authoritarianism. What the world did not understand at the time is that the Iranian government was already fully prepared to control and resist this popular uprising. In opposition to Iran's national election results announcing the reelection of Mahmoud Ahmadinejad, massive crowds of Iranian protestors took to the streets. *The Guardian* newspaper reported on the Iranian protests, "In days gone by, crushing a revolution was a lot easier. There were no mobile phones to co-ordinate street action or relay what was happening to the outside world. Even more importantly, there wasn't an Internet."[56] ICTs played a powerful role in building the initial momentum of the Green Movement and were used to engage the international community in the uprising. The capture of the death of Neda Agha-Soltan, who is believed to have been killed by a sniper's bullet, on camera is one poignant example of the engagement capacity of ICTs. The startling and graphic video that showed this young, attractive woman dying quickly went viral and became a domestic and international emblem of the protests.[57] While many of the protestors killed in the 2009 anti-government protests in Iran remained anonymous, Neda became a symbol for opposition supporters and activists in Iran, so much so that her narrative resurfaced during the 2013 Iranian elections.[58] The movement was deemed a "Twitter Revolution,"[59] and the

U.S. State Department famously contacted Twitter to request they delay a planned upgrade during the height of the protests.

ICTs were a powerful tool and force multiplier for the protestors during the Green Movement, but their potential was simply overwhelmed by Iran's tremendous mass surveillance capabilities such that the Green Movement was ultimately unsuccessful in overturning the results of the election. There has been speculation that the subsequent brutal crackdown by the Iranian authorities, the lack of hierarchical structure in the movement, or the absence of a charismatic leader for the opposition might have all contributed to the failure of the protests. A complete explanation is undoubtedly complex, but it cannot be discounted that the ability of the Iranian Government to monitor every phone call, email, text, social media message, to track the GPS location of activists carrying cellphones, and to shut down the Internet at will had a significant impact on the outcome of the Green Movement. Unlike in Ukraine in 2004, in Iran, the ruling regime had the advantage. Communication is power; if an authoritarian regime can control communication more quickly and more effectively than those that seek to oppose them, they retain an absolute advantage in the power balance between citizen and state.

When protestors filled the streets of Tehran, Iran's government was capable of controlling and monitoring every modern mode of communication available to the protestors.[60] The previous year, Iran had acquired surveillance capabilities from Siemens AG and Nokia Corporation,[61] which enabled the security services to build "one of the world's most sophisticated mechanisms for controlling and censoring the Internet, allowing it to examine the content of individual online communications on a massive scale."[62] The technology was originally sold to Iran under the "lawful intercept" concept that allows telecom companies to intercept data for the purposes of law enforcement working to stop child pornography, terrorism, drug trafficking and other illegal activities.[63] But as is possible with all dual-use technologies, particularly in countries without proper oversight and democratic institutions, these surveillance capabilities were also used to spy on dissidents and protestors in Iran who were detained and tortured as a result of inter-

Communication is power; if an authoritarian regime can control communication more quickly and more effectively than those that seek to oppose them, they retain an absolute advantage in the power balance between citizen and state.

cepted communications. The case of Saleh Hamid in 2008 provides indication of the regime's surveillance capabilities prior to the Green Movement. Hamid, a university student, was arrested and beaten after being accused of spreading propaganda about the ruling regime. Evidence presented against him included transcripts of his own cellphone calls.[64]

Continuing to hone their ability to control and monitor communications after the events of 2009, the Iranian government spent an estimated 500 million dollars in 2010-2011 to combat "what it termed a 'Soft War' being waged against the regime by its perceived enemies via media and online activities."[65] In January 2011, Iran established its first cyber police unit. The head of Tehran's new unit said of their mission, "the growth and influence of the Internet indicate the rapidly growing inclination towards cyberspace, but information technology entails both threats and opportunities."[66] The result of the real threat of arrest and torture for producing online content that criticizes the regime and extensive surveillance has led to the current state of online activity in Iran to be described by Freedom House in this way:

> Self-censorship is extensive, particularly on political matters. The widespread arrests and harsh sentences meted out to reporters and activists after the 2009 elections, as well as perceptions of pervasive surveillance, have increased fear among online journalists and bloggers. Many of them either abandoned their online activities or use pseudonyms. The result has been a palpable drop in the amount of original content being produced by users based inside the country.[67]

Until citizens living under authoritarianism are provided the tools and training necessary to circumvent mass surveillance technologies and regain a technological advantage in private communication, it is unlikely that any popular protest will succeed as they did during Ukraine's Orange Revolution.

As ICTs provide liberating opportunities for civil society to claim power from the state in authoritarian regimes, those regimes are working ceaselessly to find new tools and strategies to retain the power advantage and hold onto it with an iron fist.

There has been evidence to suggest that Iran's mass surveillance of online activities and cellphone-based communications and the consequences of information obtained from that surveillance since the Green Movement have deterred Iran's civil society from organizing via the Internet. Until citizens living under authoritari-

anism are provided the tools and training necessary to circumvent mass surveillance technologies and regain a technological advantage in private communication, it is unlikely that any popular protest will succeed as they did during Ukraine's Orange Revolution.

AUTHORITARIAN REGIMES ARE WATCHING AND LEARNING

The timing of known acquisition dates of mass surveillance technologies by other repressive regimes in the Middle East and North Africa suggests that these regimes were watching and learning from the events of 2009 in Iran, just as Iran had been watching and learning from the 2004 Orange Revolution in Ukraine. One of the first pieces of dated evidence that provides proof of regimes acquiring mass surveillance technologies in the region is from 2010 in Egypt.

The timing of known acquisition dates of mass surveillance technologies by other repressive regimes in the Middle East and North Africa suggests that these regimes were watching and learning from the events of 2009 in Iran, just as Iran had been watching and learning from the 2004 Orange Revolution in Ukraine.

On January 25, 2011, the popular demonstrations that ultimately took down the Mubarak regime began in Tahrir Square. As the world watched the protesters grow in number and in fervor, the Egyptian State Security Investigations (SSI) services were exploring revolutionary ways to monitor the protestors' every text, phone call and movement. Just months before the protests erupted, and unbeknownst to the international community and the Egyptian people, President Mubarak had been testing a new technology that could effortlessly monitor every type of modern communication happening inside the country from Skype calls to Tweets. On June 29, 2010, Mubarak received an offer from the company Gamma International UK Limited for "'FinSpy' software, hardware, installation and training to the SSI for €287,000."[68] Human rights activists found the documents linking Egypt's regime to FinSpy in the headquarters of the SSI.[69] The SSI had just completed a satisfactory trial of the software in December 2010 and was prepared to purchase FinFisher, a transaction that was averted only by the events of the Arab Spring. The company behind FinSpy was Gamma International, headquartered in the town of Andover in the United Kingdom. The documents

that were uncovered confirmed that the British company had provided this mass surveillance technology to the Mubarak regime, a government that in the previous year was reported by Human Rights Watch to have "regularly engaged in torture in police stations, detention centers, and at points of arrest" and "also 'disappeared' young political activists for several days."[70]

At the time of the 2011 revolution in Libya, Muammar el-Qaddafi's regime was in talks with French company Amesys and the Boeing Company's Narus to add to existing capabilities, "tools to control the encrypted online-phone service Skype, censor YouTube videos and block Libyans from disguising their online activities by using 'proxy' servers."[71] Amesys was revealed to have provided Qaddafi with a sophisticated suite of Internet monitoring equipment that allowed the regime to spy on activists and monitor their online activities. Amesys produces a technology known as EAGLES, described in its own promotional materials released by WikiLeaks as a "core technology … designed to help law enforcement agencies and intelligence organizations to reduce crime levels, to protect from terrorism threats and to identify new incoming security danger."[72] These were not the only activities for which Qaddafi's intelligence services used the technology: additionally, Qaddafi secretly monitored the communications of activists, intellectuals, and opposition figures both within Libya's borders and beyond. Exiles living in the United States and in Britain were targeted by this technology.[73] As was reported by OWNI and Wikileaks after the fall of Libya's strongman, a manual was discovered in the offices of the security services in which was found "pseudonyms and email addresses of Libyan opposition figures—as well as those of two U.S. officials, a British lawyer and dozens of employees of a Tunisian bank—appear by name in a manual for a 'massive Internet surveillance' system known as the Eagle system, which was created in March 2009 by Amesys employees."[74]

History demonstrates that since the middle of the nineteenth century, citizens and sovereigns have been engaged in a cat and mouse style chase to harness the power of new communication technologies to their own advantage, a process that will continue unabated in the years and decades to come.

Other authoritarian rulers like Gurbanguly Berdimuhamedov of Turkmenistan and Omar al-Bashir of Sudan have continued to watch and learn. Although available evidence is not irrefutable on the timing of these regimes' acquisition of mass surveil-

lance technologies, data suggests that in response to the Arab Spring uprisings, Turkmenistan acquired the powerful FinSpy technology in 2012[75] and new evidence surfacing in June 2013 revealed that Sudan now has Blue Coat surveillance technology.[76]

ICTS ARE NOT A SILVER BULLET—BUT THEY STILL PACK A PUNCH

History demonstrates that since the middle of the nineteenth century, citizens and sovereigns have been engaged in a cat and mouse style chase to harness the power of new communication technologies to their own advantage, a process that will continue unabated in the years and decades to come. It is worthwhile to recall that the Solidarity Movement in Poland and the anti-apartheid movement in South Africa succeeded before the era of ICTs.[77] Chile's Pinochet and Marcos' regime in the Philippines were overthrown through highly organized and strategic non-violent conflicts before Facebook and cellphones had proliferated around the world.[78] However, history also demonstrates that populations are unlikely to revert to a simpler technological age of communications to respond to the threat of mass surveillance technologies. Otpor![79] succeeded in its time because it relied on the communication tools and strategies that were appropriate for the time; today's popular protests demand new tools and new strategies.

It is true that a single photo of a human rights abuse is not always going to be enough of a catalyst to overthrow a regime, but when the forces of economic frustration, disillusion with corrupt officials, and social cohesion collide, a photo or a video may be all a society needs to unleash the anger and tension already boiling just below the surface.

ICTs are a powerful force multiplier for non-violent civil resistance movements and have played a tremendous role in the popular protests of recent years. Just as the video of Neda in Iran rallied protestors during the Green Movement in 2009, it was also a startling and graphic video that sparked the revolutionary movements the world watched unfold in 2011. On December 17, 2010, Mohamed Bouazizi, a twenty-six year-old street vendor in Tunisia, was caught on tape as he set himself on fire after police seized his produce and publicly humiliated him. The visual narrative of Bouazizi as a martyr quickly spread through Al-Jazeera, YouTube, Facebook, and Twitter, playing into existing

cultural narratives of martyrdom and social justice in Tunisia, and allowing the story of Bouazizi to evolve into the revolution that eventually toppled the country's long ruling regime.[80] Just six months prior to Bouazizi's self-immolation, twenty-eight year-old Khaled Saeed was pulled from an Internet café in Alexandria, Egypt and beaten to death by two Egyptian police officers. Saeed was found to have shared a video of the police officers "divvying up seized narcotics and cash"[81] with friends; the police officers that murdered Saeed were implicated in the video. Saeed's family acquired a photo of his disfigured and beaten body that went viral[82] and his story became a rallying cry for the protests that unseated the seemingly unshakable Hosni Mubarak.

Writing just before the events of the Arab Spring, Evgeny Morozov argued, "tweets don't overthrow governments, people do."[83] This point is hard to dispute, but he also goes on to say that "neither the Iranian nor the Burmese regime has crumbled under the pressure of pixelated photos of human rights abuses circulated on social networking sites."[84] It is true that a single photo of a human rights abuse is not always going to be enough of a catalyst to overthrow a regime, but when the forces of economic frustration, disillusion with corrupt officials, and social cohesion collide, a photo or a video may be all a society needs to unleash the anger and tension already boiling just below the surface. The photo of Khaled Saeed's mangled body and the video of Mohamed Bouazizi's self-immolation didn't overthrow President Mubarak and President Ali, but they were the sparks that ignited the years of accumulated tension, desperation, and frustration of the Egyptian and Tunisian people.

The consequence of mass surveillance is the loss of the liberating potential of these tools, the destruction of trust, and the degradation of privacy that weakens civil society and significantly inhibits the development of democracy.

The Internet was the medium that drew the world's attention to the social injustices the people of Tunisia and Egypt were subject to and the world watched as they collectively united to overthrow their long entrenched, corrupt governments. Al Jazeera quoted a protestor in Tunisia as remarking that, "we could protest for two years here, but without videos no one would take any notice of us."[85] In 1981 there were seventeen attempts of self-immolation in Red Square, "none of them known to the outside world, and more important, to the Soviet population."[86] It can only be speculated as to what impact these events would have had if

the world and the rest of the Soviet Union had watched them transpire on YouTube as the world was able to witness Bouazizi's desperate last act of defiance in Tunisia.

Secrecy is a powerful tool of authoritarian regimes and it has been used by these regimes as a tool of repression and fear. The Internet, cellphones and social media empower average citizens to pierce the veil of secrecy and shed light on their government's actions. Once that secrecy is broken, a space is created for activists, journalists and citizens to demand accountability from their government and to shift the balance of power away from the state and into the hands of the people. These tools are force multipliers that allow well-organized, non-violent civil resistance movements to create cracks and to exploit them[87] in new and powerful ways. The consequence of mass surveillance is the loss of the liberating potential of these tools, the destruction of trust, and the degradation of privacy that weakens civil society and significantly inhibits the development of democracy.

CHANGING THE COURSE OF THE ORWELLIAN REALITY

In 2010 Secretary of State Hillary Clinton delivered a landmark speech on Internet freedom in which she said,

> Amid this unprecedented surge in connectivity, we must also recognize that these technologies are not an unmitigated blessing. These tools are also being exploited to undermine human progress and political rights. Just as steel can be used to build hospitals or machine guns, or nuclear power can either energize a city or destroy it, modern information networks and the technologies they support can be harnessed for good or for ill.[88]

She recalled the days of Eleanor Roosevelt and the Universal Declaration of Human Rights and said of that legacy, "so as technology hurtles forward, we must think back to that legacy. We need to synchronize our technological progress with our principles."[89] However, in her speech she made no mention of the mass surveillance industry. Just a year after Secretary Clinton delivered this speech, it was found that the Assad regime in Syria was using California-based Blue Coat surveillance in that country's bloody civil war.[90]

Many have warned of the terrifying arrival of the Orwellian nightmare. But the harsh reality is that for millions of people around the world who are living under authoritarianism, the proliferation of western-made mass surveillance technologies has already made that nightmare a reality. One of the greatest threats to citizens living under authoritarianism today

is the technology developed by the very citizens who enjoy the freedom and opportunity to engage in innovation and entrepreneurship in western democracies. If democratic states aspire to support the freedom and human rights of people across the globe, the same democracies responsible for developing both these concurrently liberating and repressive tools have a responsibility to control their sale to regimes with poor human rights records and to take measures to assist civil society in authoritarian regimes to counter the overwhelming cyber-force of mass surveillance technologies. What complicates these efforts though is the revelation that the government of the United States is itself using mass surveillance to monitor its own populace through the now well-known PRISM program of the National Security Agency. Americans must also decide what example they wish to be for the rest of the world and how to reconcile mass surveillance with the need to protect privacy and promote trust so as to ensure the perpetuation of American democracy.

It is still possible for citizens living under authoritarian regimes utilizing mass surveillance technologies to win in a non-violent struggle against the state, but it will require a different strategy, new tools and innovative techniques to succeed. In 2006, the democratic west put Facebook in the hands of the people and just a few years later armed their repressors with FinFisher. Today, mass surveillance technologies employed by authoritarian regimes and democracies alike are the most pressing challenge to democracy; this challenge is the call our generation must answer to advance human rights and freedom across the globe. ***f***

ENDNOTES

1 The final death toll remains a mystery as eyewitness reports and official government statements on the incident paint incongruous versions of the truth.
2 "Turkmenistan: 100 Die in Arms Depot Explosion, Says Russian Media Report," EurasiaNet. July 8, 2011, <http://www.eurasianet.org/node/63829> (accessed June 22, 2013).
3 Ibid.
4 Ibid.
5 Ibid.
6 At the time of writing, this website was blocked in Turkmenistan.
7 "Turkmenistan: Death Toll Reaches 200 in Arms Depot Explosion," *EurasiaNet*. July 8, 2011, <http://www.eurasianet.org/node/63834> (accessed June 22, 2013).
8 "After Denials, Turkmen Officials Admit Blast Caused Casualties," Radio Free Europe. July 11, 2011, <http://www.rferl.org/content/turkmen_officials_admit_blast_caused_casualties/24261862.html> (accessed April 18, 2013).
9 "Freedom of the Press 2013," Freedom House, <http://www.freedomhouse.org/sites/default/files/Global%20and%20regional%20tables.pdf> (accessed December 26, 2013).
10 Ibid.

11 Malcolm Gladwell, "Small Change: Why the revolution will not be tweeted," *The New Yorker,* October 4, 2010, <http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell> (accessed June 28, 2013).
12 Larry Diamond, "Liberation Technology." *Journal of Democracy* 21(3) (2010): 70.
13 Alec Ash, "Adam Roberts on Civil Resistance," *The Browser,* December 8, 2011, <http://old.thebrowser.com/interviews/adam-roberts-on-civil-resistance> (accessed July 16, 2013).
14 Peter Ackerman and Jack Duvall, *A Force More Powerful: A Century of Non-Violent Conflict* (New York: Palgrave, 2000), 62.
15 Alexis C. Madrigal, "The First Long-Distance Telegraph Message, Sent This Day in 1844: 'What Hath God Wrought?'," *The Atlantic,* May 24, 2013, <http://www.theatlantic.com/technology/archive/2013/05/the-first-long-distance-telegraph-message-sent-this-day-in-1844-what-hath-god-wrought/276226/> (accessed June 28, 2013).
16 Morgan Marquis-Boire, "From Bahrain With Love: FinFisher's Spy Kit Exposed?," University of Toronto and Munk School for International Affairs, Number 9, 2012, <https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/> (accessed June 26, 2013).
17 Barton Gellman and Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *Washington Post*, June 6, 2013, <http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html> (accessed December 26, 2013).
18 Morgan Marquis-Boire, "From Bahrain With Love: FinFisher's Spy Kit Exposed?," University of Toronto and Munk School for International Affairs, Number 9, 2012, <https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed> (accessed June 26, 2013).
19 Vernon Silver, "CyberAttacks on Activists Traced to FinFisher Spyware of Gamma," *Bloomberg*, July 25, 2012, <http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html> (accessed June 29, 2013).
20 Sixteen of the previous servers found in CitizenLab's scan did not show up and were suspected to have been moved to avoid detection.
21 Morgan Marquis-Boire, "For Their Eyes Only: The Commercialization of Digital Spying," University of Toronto and Munk School for International Affairs, 2013, <http://munkschool.utoronto.ca/canadacentre/research/for-their-eyes-only-the-commercialization-of-digital-spying/> (accessed May 18, 2013).
22 Irwin Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding,* (Monterey: Brooks/Cole Publishing Company, 1975), 237.
23 Julie Cohen, "What Privacy is For," *Harvard Law Review* 126 (2013): 1904.
24 Paul Dourish and Ken Anderson, "Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena," *Human Computer Interaction* 21(3) (2006), 322.
25 Ibid. 322.
26 Julie Cohen, "What Privacy is For," *Harvard Law Review* 126 (2013): 1905.
27 Dourish and Anderson, 332.
28 Ibid.
29 Charles D. Raab, "Policing Cyberspace: Privacy and Surveillance," in *The Governance of Cyberspace,* edited by Brian D. Loader. (New York: Routledge, 2004), Kindle edition,153.
30 Ibid. 154.

31 Ibid.
32 John Locke, *Two Treatises of Government,* (MacMay, 2009), Kindle edition, 10.
33 William Mishler and Richard Rose, "Trust, Distrust, and Skepticism: Popular Evaluations of Civil and Political Institutions in Post-Communist Societies," *The Journal of Politics* 59(2) (1997): 419.
34 Ibid.
35 Robert Putnam, Robert Leonardi, and Rafaella Y. Nanett, *Making Democracy Work: Civic Traditions in Modern Italy,* (Princeton and Chichester: Princeton University Press, 1993), 111.
36 Ibid.111.
37 Ibid. 165.
38 Kenneth Newton, "Trust, Social Capital, Civil Society, and Democracy," *International Political Science Review* 22:2 (2001): 205.
39 Ibid. 207.
40 Ibid.
41 Ibid. 211.
42 Ibid.
43 Mishler and Rose, 420.
44 Francis Fukuyama, "Social Capital, Civil Society and Development," *Third World Quarterly* 22:1 (2001) 12.
45 Ibid.
46 Thomas Schelling as quoted in Ackerman and Duvall, "People Power Primed: Civilian Resistance and Democratization," 42-47.
47 Ibid.
48 Joshua Goldstein, "The Role of Digital Networked Technologies in the Ukrainian Orange Revolution," *Internet and Democracy Case Study Series* 14 (2007), 3.
49 Myroslaw J. Kyj, "Internet use in Ukraine's Orange Revolution," *Business Horizons,* 49(1) (2006): 9.
50 Anders Aslund and Michael McFaul, *Revolution in Ukraine: The Origins of Ukraine's Democratic Breakthrough,* (Washington, D.C.: Carnegie Endowment for International Peace, 2006), 110.
51 Joshua Goldstein, "The Role of Digital Networked Technologies in the Ukrainian Orange Revolution," *Internet and Democracy Case Study Series* 14 (2007), 9.
52 Aslund and McFaul, 216.
53 Ibid. 109.
54 Ibid. 110.
55 Ibid. 110.
56 Haroon Siddique, "Technology makes crushing revolutions a lot harder," *The Guardian (London) - Final Edition,* June 19, 2009, 12.
57 Nazila Fathi, "In a Death Seen Around the World, a Symbol of Iranian Protests," *The New York Times*, June 13, 2009, <http://www.nytimes.com/2009/06/23/world/middleeast/23neda.html?_r=0> (accessed June 10, 2013).
58 Saeed Kamali Dehghan, "Iran elections: death of Neda Agha-Soltan haunts voters," *The Guardian (London) - Final Edition*, June 13, 2013, <http://www.theguardian.com/world/2013/jun/13/iran-elections-neda-agha-soltan> (accessed June 15, 2013).
59 Jared Keller, "Evaluating Iran's Twitter Revolution," *The Atlantic,* June 18, 2010, <http://www.theatlantic.com/technology/archive/2010/06/evaluating-irans-twitter-revolution/58337/> (accessed May 20, 2013).
60 Robert Worth and Nazila Fathi, "Protests Flare in Tehran as Opposition Disputes

Vote," *New York Times*, June 13, 2009, <http://www.nytimes.com/2009/06/14/world/middleeast/14iran.html?pagewanted=all> (accessed June 15, 2013).

61 Christopher Rhoads and Loretta Chao, "Iran's Web Spying Aided By Western Technology," *Wall Street Journal*, June 22, 2009, <http://online.wsj.com/news/articles/SB124562668777335653> (accessed June 15, 2013).

62 Ibid.

63 Ibid.

64 Steve Stecklow, "Foreign companies pitched real-time surveillance gear to Iran," *NBC News,* December 5, 2012, acces <http://investigations.nbcnews.com/_news/2012/12/05/15701843-foreign-tech-companies-pitched-real-time-surveillance-gear-to-iran?lite> (accessed June 20, 2013).

65 "Freedom on the Net 2012." Freedom House, <http://www.freedomhouse.org/report/freedom-net/freedom-net-2012> (accessed May 18, 2013).

66 "1st Cyber Police Unit Launched in Iran,"*Press TV*, January 24, 2011, accessed June 15, 2013, http://www.presstv.com/detail/161659.html.

67 "Freedom on the Net 2012."

68 Karen McVeigh, "Britain's Middle East links: Egypt: Firm offered web spying software," *The Guardian (London) - Final Edition,* April 28, 2011, <http://www.theguardian.com/technology/2011/apr/28/egypt-spying-software-gamma-finfisher> (accessed May 20, 2013).

69 Ibid.

70 "World Report 2011: Egypt," Human Rights Watch, <http://www.hrw.org/world-report-2011/egypt> (accessed May 18, 2013).

71 Paul Sonne and Margaret Coker, "Firms Aided Libyan Spies," *Wall Street Journal*, August 30, 2011, <http://online.wsj.com/news/articles/SB10001424053111904199404576538721260166388> (accessed May 18, 2013).

72 Amesys, "EAGLE GLINT Operator Manual," (2009), <http://wikileaks.org/spyfiles/docs/amesys/100_extracts-from-the-eagle-glint-operator-manual-with-more.html> (accessed June 10, 2013).

73 Vernon Silver, "CyberAttacks on Activists Traced to FinFisher Spyware of Gamma," *Bloomberg*, June 25, 2012, <http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html> (accessed June 10, 2013).

74 Jean Marc Manach, "Exclusive: How Gaddafi Spied on the Fathers of the New Libya," *owni.eu,* December 1, 2011, <http://owni.eu/2011/12/01/exclusive-how-gaddafi-spied-on-the-fathers-of-the-new-libya/> (accessed May 20, 2013).

75 Morgan Marquis-Boire, Bill Marczak, and Claudio Guarnieri, "The Smartphone who loved me: FinFisher goes mobile?" Citizen Lab and Canada Center for Global Security Studies, Munk School of Global Affairs, University of Toronto, Number 11, 2012, <http://munkschool.utoronto.ca/canadacentre/research/the-smartphone-who-loved-me-finfisher-goes-mobile/> (accessed June 10, 2013).

76 Ellen Nakashima, "Web monitoring devices made by U.S. firm Blue Coat detected in Iran, Sudan," *Washington Post,* July 8, 2013, <http://www.washingtonpost.com/world/national-security/report-web-monitoring-devices-made-by-us-firm-blue-coat-detected-in-iran-sudan/2013/07/08/09877ad6-e7cf-11e2-a301-ea5a8116d211_story.html> (accessed July 9, 2013).

77 Ibid.

78 Ibid.

79 Otpor! was a non-violent civil resistance movement in Serbia opposing the regime of Slobodan Milosevic.

80 Jeffry R. Halverson, Scott W. Ruston, and Angela Trethewey, "Mediated Martyrs of the Arab Spring: New Media, Civil Religion, and Narrative in Tunisia and Egypt," *Journal of Communication* 63 (2013): 312.
81 Ernesto Londono, "Egyptian man's death became symbol of callous state," *Washington Post*, February 9, 2011, <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/08/AR2011020806360.html> (accessed June 18, 2013).
82 Ibid.
83 Evgeny Morozov, "Think again the internet: they told us it would usher in a new era of freedom, political activism, and perpetual peace. They were wrong," *Foreign Policy* (2010), <http://www.foreignpolicy.com/articles/2010/04/26/think_again_the_internet#sthash.fMb5PZYj.dpbs> (accessed June 20, 2013).
84 Ibid.
85 Ryan Yasmine, "How Tunisia's revolution began," *Al Jazeera*, January 26, 2011, <http://www.aljazeera.com/indepth/features/2011/01/2011126121815985483.html> (accessed June 25, 2013).
86 Stephen Kotkin, *Armageddon Averted: The Soviet Collapse 1970-2000, Updated ed.* (Oxford; New York: Oxford University Press, 2008), 45.
87 "Civil Resistance: A First Look," International Center on Nonviolent Conflict, released 2010, <http://civilresistance.net> (accessed December 27, 2013).
88 Hillary Clinton, "Remarks on Internet Freedom," U.S. Department of State, January 21, 2012, <http://www.state.gov/secretary/rm/2010/01/135519.htm.>
89 Ibid.
90 Jennifer Valentino-Devries, Paul Sonne, and Nour Malas, "U.S. Firm Acknowledges Syria Uses Its Gear to Block Web," *Wall Street Journal,* October 29, 2011, <http://online.wsj.com/news/articles/SB10001424052970203687504577001911398596328> (accessed December 26, 2013).