Center for Technology Innovation at BROOKINGS

December 14, 2011

Wire Design - Collage of city pedestrians and surveillance cameras.

Recording Everything: Digital Storage as an Enabler of Authoritarian Governments

John Villasenor

EXECUTIVE SUMMARY

John Villasenor is a nonresident senior fellow in Governance Studies and in the Center for Technology Innovation at Brookings. He is also professor of electrical engineering at the University of California, Los Angeles.

Within the next few years an important threshold will be crossed: For the first time ever, it will become technologically and financially feasible for authoritarian governments to record nearly everything that is said or done within their borders – every phone conversation, electronic message, social media interaction, the movements of nearly every person and vehicle, and video from every street corner. Governments with a history of using all of the tools at their disposal to track and monitor their citizens will undoubtedly make full use of this capability once it becomes available.

The Arab Spring of 2011, which saw regimes toppled by protesters organized via Twitter and Facebook, was heralded in much of the world as signifying a new era in which information technology alters the balance of power in favor of the repressed. However, within the world's many remaining authoritarian regimes it was undoubtedly viewed very differently. For those governments, the Arab Spring likely underscored the perils of failing to exercise sufficient control of digital communications and highlighted the need to redouble their efforts to increase the monitoring of their citizenry.

Technology trends are making such monitoring easier to perform. While the domestic surveillance programs of countries including Syria, Iran, China, Burma, and Libya under Gadhafi have been extensively reported, the evolving role of digital storage in facilitating truly pervasive surveillance is less widely recognized. Plummeting digital storage costs will soon make it possible for authoritarian regimes to not only monitor known dissidents, but to also store the complete set of digital data associated with everyone within their borders. These enormous databases of captured information will create what amounts to a surveillance time machine, enabling state security services to retroactively eavesdrop on people in the months and years before they were designated as surveillance targets. This will fundamentally change the dynamics of dissent, insurgency and revolution.

The coming era of ubiquitous surveillance in authoritarian countries has important consequences for American foreign policy as well, impacting issues as diverse as human rights, trade, nuclear nonproliferation, export control, and intellectual property security.

Introduction

When Moammar Gadhafi's forces lost control of Tripoli in August 2011, the Libyan state surveillance apparatus was exposed for ordinary Libyans and the rest of the world to see. As described in an August 30, 2011 *Wall Street Journal* article,[1] companies found to have supplied communications interception and monitoring gear to Libya include French company Amesys, the Chinese telecommunications giant ZTE, and a small South African firm called VASTech. This equipment enabled Libya's state security apparatus to capture and archive "30 to 40 million minutes"[2] of telephone conversations every month and to regularly read e-mails exchanged among activists.

The Gadhafi regime was unusual among dictatorships only in that its internal spying activities were so thoroughly unmasked, not that they were occurring. There is ample evidence that other authoritarian regimes are embracing the extensive use of surveillance technology to track their own citizens as well. For example, the Syrian government under President Bashar al-Assad was reportedly working to install an interception system[3] built by Italian surveillance company Area SpA, which appears to have in turn acquired and incorporated equipment and software from California-based NetApp and Blue Coat Systems, German company Utimaco, and France-based Qosmos.[4] Evidence that Blue Coat surveillance products are being used by the Burmese government has also been uncovered.[5]

The apparent presence of U.S.-built surveillance technology in countries such as Syria and Burma has led to Congressional calls for an investigation into NetApp and Blue Coat for possible American export control violations. Both companies have denied prior knowledge that their equipment was being sold inappropriately.[6]

Even when all sellers and resellers of American-built surveillance equipment follow export control regulations, governments of export-restricted countries have other avenues for building a domestic spying capability. One option is to acquire equipment such as video cameras that can fall outside the scope of American export control laws, but that can nonetheless be used for surveillance. This approach is being used by the local government in the inland Chinese city of Chongqing, which is installing a massive network of video cameras using equipment supplied in part by Cisco.[7] While the "Peaceful Chongqing" project is portrayed as an anti-crime initiative, the data it collects will clearly be of value to authorities interested in monitoring and suppressing unapproved demonstrations as well.

There is also an enormous amount of non-American surveillance technology on the international market, some made in countries that have much laxer export control standards than the United States. The Iranian government, which is subject to extensive U.S. export control restrictions, has reportedly purchased electronic communications tracking technology from by Chinese telecommunications giant Huawei.[8] Countries can also perform surveillance using homegrown technologies.

In July, officials in Beijing began requiring businesses including hotels, restaurants, and cafes to install Wi-Fi monitoring software developed by a Shanghai company under a contract from the Chinese government.[9]

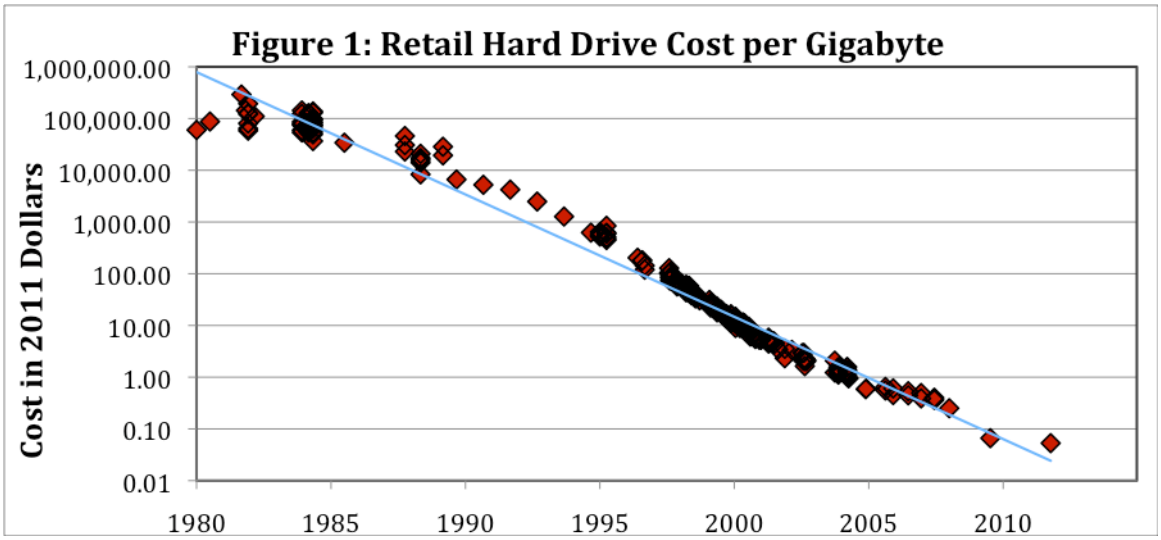
As these examples illustrate, authoritarian governments can acquire the components of a surveillance infrastructure from any number of sources across the globe or at home. In practice, therefore, an important limiting factor in the ability of these governments to employ technology in the service of their domestic spying programs is the state of technology itself. Storage technology is particularly important in this respect because it supplies the literal memory of a vast domestic surveillance apparatus.

How Much Storage Does it Take to Record Everything?

There is nothing new or noteworthy about the observation that storage costs are declining exponentially. The thresholds that get crossed along the way, however, correlate to broad shifts in the power and impact of information technology. In 1984, the commercial availability of consumer-grade 10-megabyte hard disks made it possible, as observed by the *New York Times*, to store "the equivalent of around 2,500 typed pages," removing the need "to plow through half a dozen file cabinets." By the end of the next decade, devices that could hold the digital equivalent of millions of pages of text were considered unremarkable, but storage of digital music was still a challenge. Most MP3 players of that era, noted a 1999 *New York Times* article, could "store no more than 64 minutes of high-quality music."[10]

Today's pocket-sized Apple iPod Classic can store "up to 40,000 songs, 200 hours of video, or 25,000 photos."[11] When that much information can be held in the palm of a hand, the prospect that an authoritarian government could archive the entire life of a nation no longer seems impossible. Declining storage costs will make such monitoring not only possible, but likely.

Figure 1 shows the inflation-adjusted retail cost of hard disk storage on a dollars per gigabyte basis since 1980.[12] Over the past three decades, storage costs have declined by a factor of 10 approximately every 4 years,[13] reducing the per-gigabyte cost from approximately $85,000 (in 2011 dollars) in mid-1984[14] to about five cents today.[15] In other words, storage costs have dropped by a factor of well over one million since 1984. Not surprisingly, that fundamentally changes the scale of what can be stored.



So what, exactly would it take to store everything? The answer depends in part on the nature of the information. Location data is far less voluminous than audio from phone calls, which in turn requires much less storage than video.

Location data, which is readily obtained from mobile phones, Wi-Fi connections, and GPS receivers, can already easily be archived. It takes fewer than 75 bits (ones and zeros) to pinpoint a person's location anywhere on the earth to an accuracy of about 15 feet.[16] The information identifying the location of each of one million people to that accuracy at 5-minute intervals, 24 hours a day for a full year could easily be stored in 1,000 gigabytes, which would cost slightly over $50 at today's prices. For 50 million people, the cost would be under $3000.

The audio for all of the telephone calls made by a single person over the course of one year could be stored using roughly 3.3 gigabytes.[17] On a per capita basis, the cost to store all phone calls will fall from about 17 cents per person per year today to under 2 cents in 2015. For a country like Syria, which has a population of 15 million people over the age of 14,[18] the current cost to purchase storage sufficient to hold one year's worth of phone calls for the entire country would be about $2.5 million[19] – a high number but certainly not beyond governmental reach. If historical cost trends continue, the annual cost in 2011 dollars to purchase enough storage for Syria's government to record all calls made in that country will fall to about $250,000 by 2016 and to about $25,000 by 2020. Iran has an over-age-14 population of 59 million,[20] so the corresponding cost to the Iranian government to record all calls in Iran would be about four times higher than in Syria. Cost will soon be no object for internal security services wishing to store everything said on a telephone in Syria, Iran, or even in a much more populous nation such as China.

Video surveillance can generate far more data than audio surveillance. The storage requirements for video depend on factors including the number of cameras used, the resolution of the images and the number of image frames per second

captured. At a relatively slow five frames per second, a fairly high-resolution[21] traditional video surveillance camera might generate[22] about 1 megabit per second of data. By contrast, full-motion, true "high definition"[23] video at 30 frames per second can produce anywhere from about 2 to 5 or more megabits per second.[24]

Cities around the world are increasingly deploying extensive camera systems to capture vehicle license plate numbers. As of early 2011, there were over 4000 such cameras in England and Wales providing continuous license plate data for traffic for cities including London, Birmingham, and Manchester.[25] Washington D.C. has a network of 73 license plate cameras.[26] New York uses a combination of over 100 cameras mounted at fixed roadside locations and an additional 130 cameras affixed to police cars.[27] Plate reading cameras are also being used in Canada, Australia, and India.

The deployments listed above are occurring in countries with robust ongoing debates regarding the balance of privacy and security. Privacy concerns have led to limitations on the length of time that plate data is retained – 72 hours, for example, in the case of Toronto[28] and three years for the system in Washington.[29] In authoritarian countries, however, there is essentially no open privacy debate, and governments have little incentive not to build permanent archives of license plate tracking information.

Over the course of a full year, a system of 1,000 roadside license plate reading cameras each producing 1 megabit per second would generate image data that could be held in storage costing about $200,000. The resulting database of license plate numbers (as opposed to the images used to obtain the numbers) could be stored for a small fraction of this cost.

Memory costs do not become a major obstacle to video surveillance unless the system is truly massive. Even then, the obstacle will only be temporary. The Chinese "Peaceful Chongqing" project will utilize up to 500,000 video cameras to blanket a city with a population of 12 million,[30] corresponding to one video camera for every 24 people. If each camera in that system were to produce an average of 3 megabits per second,[31] the corresponding annual cost to purchase storage to contain this data would be about $300 million dollars – an amount that would today be prohibitive. As a result, in the near term, operators of video surveillance deployments on the scale of the Peaceful Chongqing project will have to make choices. They can opt, for example, to store high-resolution data for only a limited amount of time. Or, they can permanently archive data from all of the cameras but at a lower image quality, resolution, or frame rate.

By the latter half of the decade, storage cost trends will make the need to make such choices obsolete. By 2020 the cost to store, in high resolution, all of the video acquired by the Chongqing network will drop to a much more practical $3 million per year. On a per capita basis this corresponds to about 25 cents per person per year, an amount that could easily be budgeted or even extracted from the population being monitored through a euphemistically worded "public safety tax."

In the longer term it is also possible that authoritarian regimes will choose to

augment and eventually supplant their own storage facilities by renting storage from cloud-based storage providers. At large volumes, the current monthly cost to rent storage is roughly equivalent to the amount that would be needed to purchase it outright.[32] For countries building data archiving systems on a scale where the storage costs are a significant impediment, owning is still far more cost-effective than renting. However, when storage purchase costs decline to the point where they constitute only a small fraction of the overall costs of acquiring and maintaining an archive, rental will become a more attractive option.

Of course, building a system to actually archive and exploit all of the video from public spaces, audio from telephone conversations, and location information from mobile devices requires far more than simply obtaining the requisite amount of digital storage. The data would need to be acquired, managed, aggregated, and made accessible and searchable with appropriate analysis tools. However, the problem of managing large data sets occurs in many contexts, not just in the surveillance of people in authoritarian countries. Many of the solutions that are being developed in the commercial world for searching and analyzing data could be applied to state-sponsored surveillance as well.

What about Encryption?

In principle, encryption offers a way for opponents of authoritarian regimes to communicate securely, greatly reducing the value of intercepted data. In practice, however, codes[33] have a tendency to be much less resilient than their designers and users anticipated. In fact, the history of encryption is in many respects the story of how codes thought to be secure were cracked.

Broken codes played a prominent role in the failed 1586 plot to assassinate Queen Elizabeth and place Mary, Queen of Scots on the throne.[34] The codes produced by the German Enigma machines used during World War II were cracked by Polish and British mathematicians, providing the Allies with nearly immediate access to enormous amounts of information regarding German war plans and troop movements. The data encryption standard, known by the algorithm DES, was developed in the late 1970s through a close collaboration between IBM and the U.S. government. It was claimed to be secure by its proponents, and was widely deployed both in the United States and abroad. But in 1998, a machine designed under the auspices of the Electronic Frontier Foundation was able to break DES in 56 hours of computation.[35] Today, there are a variety of modern encryption methods that are believed to be secure. However, similar beliefs have consistently proven wrong in the past, and it seems likely that at least some of the confidence placed in today's commonly used encryption methods will someday prove to be misplaced.

Against this backdrop, dissidents in authoritarian regimes face multiple obstacles in keeping their intercepted electronic communications secure. The simplest is carelessness. Many people who have good reason to believe that their communications may be targeted for interception do not always implement

sufficient data security measures.[36]

Overconfidence with respect to the security of communications technologies is a longstanding risk. The encrypted letter written by Mary, Queen of Scots conveying her complicity in the plot against Queen Elizabeth led to her beheading after the plot was foiled.[37] Until relatively recently, Skype has often been assumed to offer secure communications. However, authorities in China, the United States, and Europe have all been reported as working on cracking the encryption used in Skype.[38] In addition, in the fall of 2011 a team of researchers from Germany, France, and the United States published a paper[39] demonstrating that Skype users are vulnerable to eavesdropping that could expose their physical location as well as information about files they are acquiring or sharing via peer-to-peer services.[40] German law enforcement agencies have also been accused of using malware to compromise Skype sessions.[41] And, as researchers at the University of North Carolina have recently demonstrated, there is a class of linguistics-based methods that could allow eavesdroppers to circumvent the encryption in Skype and other VoIP communications altogether.[42]

Even the most securely encrypted messages can be decoded if the decryption keys are compromised. This could occur through keyloggers or other malware, by informants cooperating with authoritarian governments, or by dissidents who are blackmailed, deceived, or otherwise induced to divulge information enabling message decryption.

Finally, even when codes remain secure, the very act of using them can attract attention. A resident of an authoritarian nation who goes to great lengths to encrypt his or her electronic communications may be identified as a potential threat by state security services on that basis alone. Thus, while encryption is a potentially powerful tool for opponents of authoritarian regimes, there are many obstacles to its effective use, particularly when all messages, including those that are encrypted, are intercepted.

Pervasive Monitoring and the Dynamics of Dissent

In 2008, social scientist Mohammed Ibrahrine published a paper titled "Mobile Communication and Sociopolitical Change in the Arab World" that highlighted the important role of mobile phones in "empowering and mobilizing marginalized groups" and "increasing the range of alternative actions available to individuals, opposition forces, and civil society groups."[43] It was an early observation of the now widely recognized power of mobile communications to organize dissent.

However, some aspects of the ability of information technology to shift the balance of power away from repressive regimes and in favor of their opponents are temporary. When, as has been the case, the flood of electronic information is too voluminous for authoritarian governments to capture, store, and effectively analyze in its entirety, the information advantage can indeed lie with regime opponents. It is an advantage that has recently been exploited to varying degrees of success in Tunisia, Iran, Syria, Egypt, Libya, and elsewhere.

But the ability to record everything will tilt the playing field back in favor of repressive governments by laying the foundation for a plethora of new approaches to targeting dissent. When all of the telephone calls in an entire country can be captured and provided to voice recognition software programmed to extract key phrases, and when video footage from public spaces can be correlated in real time to the conversations, text messages, and social media traffic associated with the people occupying those spaces, the arsenal of responses available to a regime facing dissent will expand. Some changes will be immediate and tactical. Instead of implementing broad social media or Internet shutdowns in response to unrest,[44] governments in possession of complete communications databases will be able to conduct more selective censorship or alteration of message traffic during periods of instability. This will provide a greater capability to shape or quell dissent.

Pervasive monitoring will provide what amounts to a time machine allowing authoritarian governments to perform retrospective surveillance. For example, if an anti-regime demonstrator previously unknown to security services is arrested, it will be possible to go back in time to scrutinize the demonstrator's phone conversations, automobile travels, and the people he or she met in the months and even years leading up to the arrest.

There are also longer-term consequences that include a thinning in the ranks of regime opponents. By definition, organized dissent requires that dissenters have the ability to exchange information. Prominent opponents of repressive governments have learned to expect tracking of their movements and interception of their phone calls and other forms of electronic communications. But when technology enables an entire country's worth of communications to be intercepted, the circle of people whom dissidents will be able to recruit to their ranks will narrow.

In addition, knowledge that communications are archived will reduce the willingness of dissidents to speak frankly even over encrypted communications. Time will often favor an authoritarian government able to store intercepted data that is initially too securely encrypted to decode. Due to some combination of advances in code-breaking, computing capabilities or intentional or unintentional compromise of decryption keys, many encrypted messages will become decodable by state security services. Awareness of the likelihood that all messages – including those that are encrypted – will eventually be read by security services will chill dissent.

Conclusions

Declining storage costs will soon make it practical for authoritarian governments to create permanent digital archives of the data gathered from pervasive surveillance systems. In countries where there is no meaningful public debate on privacy, there is no reason to expect governments not to fully exploit the ability to build databases containing every phone conversation, location data for almost every person and vehicle, and video from every public space in an entire country.

This will greatly expand the ability of repressive regimes to perform surveillance of opponents and to anticipate and react to unrest. In addition, the awareness among the populace of pervasive surveillance will reduce the willingness of people to engage in dissent.

The coming era of ubiquitous surveillance in authoritarian countries has important implications for American foreign policy. Strategies for engaging with these countries will benefit from specific consideration of the presence, growth and increasing impact of these enormous digital databases. This will impact human rights, trade, export control, intellectual property security, and the operation of multinational businesses with in-country facilities, subsidiaries, or subcontractors.

Finally, the use by authoritarian governments of systems that record everything in the complete absence of privacy considerations will lead to a long list of other unforeseen and generally negative consequences. Unfortunately, the residents of those countries, as well as the rest of us, will soon start to find out just what those consequences are.

Governance Studies
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
www.brookings.edu/governance.aspx

Editor
Christine Jacobs

Production & Layout
John S Seo

E-mail your comments to gscomments@brookings.edu

Endnotes

[1] Paul Sonne and Margaret Coker, "Firms Aided Libyan Spies," *Wall Street Journal*, August 30, 2011, http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html , retrieved November 11, 2011.
[2] Ibid.
[3] Ben Elgin and Vernon Silver, "Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear," *Bloomberg*, November 3, 2011, http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html, retrieved November 11, 2011.
[4] Following the *Bloomberg* articles, Area SpA's CEO and Utimaco have stated that they were no longer moving forward on the project in Syria. See Ivan Watson, "Cyberwar explodes in Syria," CNN, November 22, 2011, http://www.cnn.com/2011/11/22/world/meast/syria-cyberwar/index.html, retrieved November 25, 2011.
[5] Andy Greenberg, "Researchers Spot Blue Coat Web Control Gear In Another Repressive Regime: Burma," *Forbes*, November 9, 2011, http://www.forbes.com/sites/andygreenberg/2011/11/09/researchers-spot-blue-coat-web-control-gear-in-another-bad-regime-burma/, retrieved November 11, 2011.
[6] Ben Elgin and Vernon Silver, "NetApp Role in Syria Spy Project Spurs Demands for U.S. Inquiry," *Business Week*, November 11, 2011, http://www.businessweek.com/news/2011-11-11/netapp-role-in-syria-spy-project-spurs-demands-for-u-s-inquiry.html, retrieved November 12, 2011
[7] Loretta Chao and Don Clark, "Cisco Poised to Help China Keep an Eye on Its Citizens," *Wall Street Journal*, July 5, 2011, http://online.wsj.com/article/SB10001424052702304778304576377141077267316.html , retrieved November 11, 2011.
[8] Steve Stecklow, Farnaz Fassihi, and Loretta Chao, "Chinese Tech Giant Aids Iran," *Wall Street Journal*, October 27, 2011, http://online.wsj.com/article/SB10001424052970204644504576651503577823210.html , retrieved November 13, 2011.
[9] Andrew Jacobs, "China Steps Up Web Monitoring, Driving Many Wi-Fi Users Away," *New York Times*, July 25, 2011, http://www.nytimes.com/2011/07/26/world/asia/26china.html, retrieved November 12, 2011.
[10] Michel Marriott, "Digital Players Break New Ground," *New York Times*, November 18, 1999, http://www.nytimes.com/1999/11/18/technology/digital-players-break-new-ground.html, retrieved November 19, 2011.
[11] http://www.apple.com/ipodclassic/, retrieved November 19, 2011.

[12] Non-inflation-adjusted hard drive costs on a dollars per gigabyte basis were compiled by Matt Komorowski and published at http://www.mkomo.com/cost-per-gigabyte, retrieved November 13, 2011. Those data in turn were attributed to an extensive set of archival storage cost records compiled at http://ns1758.ca/winch/winchest.html. To generate the data for Figure 1, the costs listed at http://www.mkomo.com/cost-per-gigabyte were adjusted for inflation using the CPI numbers published by the Social Security Administration at http://www.ssa.gov/oact/STATS/avgcpi.html, retrieved November 13, 2011. The CPI for Q3 2011 was used as the basis for computing costs expressed in 2011 dollars. An additional data point of 5.3 cents per gigabyte as of October 2011 was added to the data at http://www.mkomo.com/cost-per-gigabyte. The October 2011 data point was based on the following article: Kim Saccio-Kent, "Seagate Barracuda XT 3TB Internal Hard Drive, $160." *PC World*, October 22, 2011, http://www.pcworld.com/article/242207/seagate_barracuda_xt_3tb_internal_hard_drive_160.html, retrieved November 13, 2011. The horizontal year labels on the figure indicate January 1 of the listed year.

[13] Based on the best-fit line to the data in Figure 1, storage costs have on average decreased by a factor of 10 every 4.2 years.

[14] Choosing any single number as "the" cost of storage at a particular time is challenging because costs are volume dependent. Larger drives are less expensive than smaller drives on a dollars-per-unit-storage basis. A reasonable indicator of cost can be obtained by averaging over the typical large drive sizes available at any snapshot in time. The mid-1984 figure of $85,000 per gigabyte was obtained by averaging prices from six different manufacturers as advertised in the May 1984 issue of *Creative Computing* magazine as reported at http://ns1758.ca/winch/winchest.html. On a dollars per megabyte basis, the advertised drives ranged from a low of US $80 (not inflation-adjusted) for a 23-megabyte drive from Pegasus to a high of $299 (not inflation-adjusted) for a 5-megabyte drive from Tecmar. The average cost in 1984 dollars for all the reported drives in the May 1984 *Creative Computing* advertisement was $177 per megabyte, or equivalently $177,000 per gigabyte. To adjust for inflation, CPI data from the Social Security Administration was used. See "Average CPI by Quarter and Year," http://www.ssa.gov/oact/STATS/avgcpi.html, retrieved November 13, 2011. The average CPI for 1985 was 106.9; as of Q3 2011 it was 223. Applying the CPI information gives a cost of $85,000 per gigabyte in 2011 dollars.

[15] As of late October 2011, 3 terabyte hard drives could be purchased for $160. A terabyte is 1000 gigabytes. See Kim Saccio-Kent, "Seagate Barracuda XT 3TB Internal Hard Drive, $160." *PC World*, October 22, 2011, http://www.pcworld.com/article/242207/seagate_barracuda_xt_3tb_internal_hard_drive_160.html, retrieved November 13, 2011.

[16] Most location tracking systems are less precise, and would therefore lead to less data and correspondingly lower storage requirements. Even when 15-foot accuracy

is obtainable, the figure of 75 bits given in the text is very conservative. In an efficiently designed system, about 46 bits would be sufficient to provide latitude and longitude information pinpointing a person's location anywhere on the earth to an accuracy of about 15 feet. A sequence of 23 bits could specify latitude to within 3.5 meters. An additional 23 bits could locate longitude to within 3.5 meters at the equator (and to increasingly better accuracy as one moves towards the poles). The total of 46 bits would therefore identify location to within an area of no more than 7 by 7 meters. This would correspond to a maximum location error equal to the distance between the center and corners of a 7-meter by 7-meter square. That distance is about 5 meters, or about 15 feet. Of course, there would also need to be storage of metadata identifying the individual associated with the location information, though if there are many location measurements for each individual the marginal contribution of the metadata to the overall storage requirements would be negligible.

[17] This calculation assumes that each person spends an average of one hour per day on the phone, and that the associated audio signal is compressed to an average rate of 20 kilobits per second.

[18] Central Intelligence Agency, World Factbook, https://www.cia.gov/library/publications/the-world-factbook/, population data retrieved November 13, 2011.

[19] The total storage requirement would be about 50,000 terabytes, which at about $50 per terabyte corresponds to a cost of $2.5 million. Additional storage efficiencies could be obtained by avoiding the redundancy of separately storing both ends of the same phone call.

[20] Central Intelligence Agency World Factbook, op. cit.

[21] There is an alphabet soup of acronyms used to describe different image resolutions. Traditionally, "D1", which is 720 by 480 pixels, has been considered high resolution in the context of video security systems.

[22] The raw data rate from such a camera would be much higher than 1 megabit per second. A compression method such as H.264 could be used to reduce the rate to approximately 1 megabit per second, though the rate could also be higher or lower than this amount depending on the desired output image quality.

[23] There are various "high definition" formats, including images with dimensions 1280 by 720 pixels (often called "720p", with the "p" indicating that the image is scanned in a progressive manner, one line after another) and 1920 by 1080 pixels (typically denoted "1080p" if progressive scanning is used or "1080i" if interleaved scanning is used). Cisco, for example offers surveillance cameras capable of producing 30 frames per second of video at resolution of 1920 by 1080 pixels. See the data sheet for the Cisco Video Surveillance 4000 Series High-Definition IP Cameras, http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps9692/ps9716/data_sheet_c78-492032.html, retrieved November 16, 2011.

[24] These rates assume the use of a compression method such as H.264.
[25] SA Mathieson, "Privacy groups take Royston's ANPR plans to ICO," *The Guardian*, June 10, 2011, http://www.guardian.co.uk/government-computing-network/2011/jun/10/royston-hertfordshire-constabulary-anpr-cctv, retrieved November 20, 2011.
[26] As reported in November 2011. See Allison Klein and Josh White, *The Washington Post*, November 19, 2011, "License plate readers: A useful tool for police comes with privacy concerns," http://www.washingtonpost.com/local/license-plate-readers-a-useful-tool-for-police-comes-with-privacy-concerns/2011/11/18/gIQAuEApcN_story.html, retrieved November 20, 2011.
[27] As reported in April 2011. See Al Baker, "Camera Scans of Car Plates Are Reshaping Police Inquiries," *New York Times*, April 11, 2011, http://www.nytimes.com/2011/04/12/nyregion/12plates.html, retrieved November 20, 2011.
[28] SA Mathieson, op. cit.
[29] Allison Klein and Josh White, op. cit.
[30] Loretta Chao and Don Clark, op. cit.
[31] 3 megabits per second would be sufficient to store full-rate (30 frames per second) video at high resolution and very good video quality (or, at frame rates below 30 frames per second, either or both of the resolution and video quality could be increased).
[32] For example, as of November 2011, at large volume (over 5000 terabytes) Amazon's "Simple Storage Service" is priced at 5.5 cents per gigabyte per month (with a reduced redundancy option available at 3.7 cents per gigabyte per month). See http://aws.amazon.com/s3/, retrieved November 19, 2011. The amount paid to rent storage for one month is about equal to the current cost to purchase it outright.
[33] Technically, a "code" is different from a "cipher." For simplicity, the term "code" is used here to both forms of encryption.
[34] Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (New York: Anchor, 1999)
[35] "Frequently Asked Questions (FAQ) About the Electronic Frontier Foundation's 'DES Cracker' Machine," Electronic Frontier Foundation, http://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_des_faq.html, retrieved November 16, 2011.
[36] For example, careless encryption clerks in World War II sometimes failed to follow some very simple procedures designed to make encoded messages harder to decrypt. See Ronald V. Layton, Jr., "Cryptography," in *World War II in Europe, an encyclopedia, Volume II*," ed. David Zabecki, (New York: Routledge, 1999), 1193.
[37] Simon Singh, op. cit.

[38] "EU aims to crack Skype encryption to listen in on criminals," *Computer Weekly*, February 23, 2009, http://www.computerweekly.com/news/2240088503/EU-aims-to-crack-Skype-encryption-to-listen-in-on-criminals, retrieved November 25, 2011.
[39] Stevens Le Blond, Chao Zhang, Arnaud Legout, Keith Ross, Walid Dabbous, "I Know Where You are and What You are Sharing: Exploiting P2P Communications to Invade Users' Privacy," retrieved from http://cis.poly.edu/~ross/papers/skypeIMC2011.pdf on November 15, 2011. Publication is undated, though the news coverage of this paper occurred in October 2011.
[40] Chloe Albanesius, "Tracking Your Location ... With Skype?" *PC Magazine*, October 25, 2011, http://www.pcmag.com/article2/0,2817,2395225,00.asp#fbid=rMxANgfm9kD, retrieved November 16, 2011.
[41] Elinor Mills, "Trojan opened door to Skype spying," *CBS News*, October 10, 2011, http://www.cbsnews.com/stories/2011/10/10/scitech/main20118260.shtml, retrieved November 16, 2011.
[42] Robert Vamosi, "Defeating Skype Encryption Without a Key," *Security Week*, June 16, 2011, http://www.securityweek.com/defeating-skype-encryption-without-key, retrieved November 25, 2011.
[43] Mohammed Ibahrine. "Mobile Communication and Sociopolitical Change in the Arab World," in *Handbook of Mobile Communication Studies*, ed. James E. Katz. Boston: MIT Press, 2008.
[44] There are many examples of government-ordered media shutdowns in authoritarian countries. See, for example, "Tehran blocks access to Facebook" *BBC News*, May 24, 2009, http://news.bbc.co.uk/2/hi/8065578.stm, retrieved November 19, 2011. See also Charles Arthur, "Egypt blocks social media websites in attempted clampdown on unrest," The Guardian, January 26, 2011, http://www.guardian.co.uk/world/2011/jan/26/egypt-blocks-social-media-websites, retrieved November 19, 2011.