Leading in the Age of Super-Transparency

Austin, Robert D.; Upton, David

Document Version
Accepted author manuscript

Published in:
MIT Sloan Management Review

Publication date:
2016

Creative Commons License
Unspecified

Citation for published version (APA):
Austin, R. D., & Upton, D. (2016). Leading in the Age of Super-Transparency. *MIT Sloan Management Review*, *57*(2), 24-32.

Leading in the Age of Super-Transparency

Robert D. Austin and David Upton

Journal article (Post print version)

This article was originally published in *M I T Sloan Management Review*, Vol 57, Issue 2, Pages 25-32.

First published online December 14, 2015.

Link to publisher: http://sloanreview.mit.edu/article/leading-in-the-age-of-super-transparency/

Uploaded to Research@CBS: Januar 2016

Living and Leading in an Era of Super-Transparency

Robert D. Austin, Copenhagen Business School

David M. Upton, Said Business School, University of Oxford

Introduction

When nine year-old Martha Payne, a student in Argyll, Scotland, decided to start a blog in April of 2012, she had no idea what a stir she would soon cause. Something she had noticed offended her youthful sense of justice: published descriptions of the lunches her school offered students seemed a lot better than what turned up on their plates. Embracing a cause expressed in her newly adopted screen name, "VEG" (short for "Veritas Ex Gustu," which means "Truth from tasting"), and with tech support from her dad, Martha set out to photograph and rate her lunches, and to post the reviews to a blog she christened "NeverSeconds."

Soon Martha was photographing, rating, and reviewing every day. The amount of food emerged as an early concern. "I'd have enjoyed more than 1 croquette," she said, in a post from the first week; "I'm a growing kid and I need to concentrate all afternoon and I can't do it on one croquette. Do any of you think that you could?"

Readers didn't. "My toddler eats more than that," one observed. Others questioned the food's nutritional value, using words like "pathetic," "rubbish," and "disgraceful." When celebrity chef Jamie Oliver made supportive remarks in the UK media about Martha's project, newspapers covered the story, calling Argyll school lunches "miserable-looking." Riding a wave of publicity, NeverSeconds logged two million hits in its first six weeks. Martha started a

fund to build lunchrooms for kids in places in the world where they don't have school lunches.

Then, suddenly, six weeks in, the initiative screeched to a halt. Martha explained in an entry titled "Goodbye": "This morning in maths I gotten taken out of class by my head teacher and taken to her office. I was told that I could not take any more photos of my school dinners because of a headline in a newspaper today." Her dad also posted, noting that Martha's charity efforts, which had raised £2000, would end, and thanking the school for being supportive. The decision to shut down NeverSeconds had come, he explained, from the Argyll and Bute Council.

A firestorm ensued. Within 24 hours, readers deposited 2,416 new comments on NeverSeconds, most expressing outrage. "I am livid that Argyll and Bute Council have banned you," said one; "ridiculous behavior by Argyle & Bute council" opined another. Protests flooded the Argyle and Bute Council website. Someone started a petition (argyle-and-bute-council-lift-the-ban-on-the-never-seconds-blog-about-school-dinners). NeverSeconds logged another million hits. The Twitter hashtag #MyLunchforMartha trended, and a dedicated FaceBook page amassed comments. Half a world away, *Wired* magazine published a story on its website headlined "9-Year-Old Who Changed School Lunches Silenced by Politicians."

One day later, the Argyll and Bute Council reversed its decision. The shell-shocked Council struggled to explain that it had merely been trying to protect the wounded feelings of cafeteria workers, but the world didn't seem to care. An army of social media peeps that had coalesced, more or less instantly, united by indignation over the blog's shutdown, celebrated within their new community. Martha's fund raising and campaign for better lunches resumed

stronger than ever, as she appeared on television with Jamie Oliver. NeverSeconds garnered "Best Blog of the Year" awards.

The pattern that underlies this story has become common. Every day, images or events with potential to incite passions get captured digitally, posted to the web, and "go viral." In Martha's case, it started with innocuous food photos, but it could just as easily have been an audio recording of an ascerbic customer service rep on a phone call (as happened when a customer called Comcast last year) or a video capture of police seeming overly zealous in arresting a student for jay-walking (as happened in Austin, Texas recently). Via social media, people share with friends or followers, who share with more people. At dazzling speed, something that had constituted not the barest glimmer of a cause, instantly materializes into a powerful one, propelled by a nascent virtual community. And some unsuspecting party -- like the Argyll and Bute Council (or Comcast, or the Austin, Texas police department) -- suddenly gains a huge, new problem.

Powerful causes have always sprung from evocative images and events. But they have not always arisen with such speed or from such obscure, unexpected, often far away, sources. In the past, controversies brewed within physical gatherings of people, and were transmitted, if they grew active enough, by a countable number of media outlets, which also served as gatekeepers (applying journalistic standards, for example). Today's controversies, in contrast, spring to life in uncountable, overlapping on-line communities and get distributed via flash-networks of unaccountable independent agents sharing information in real time. There are no gatekeepers. This capacity to generate causes and controversies almost instantly is, perhaps, the most salient aspect of what we call the "super-transparent society," which has rapidly become a new norm. Because this has happened so fast, most people, especially leaders of

organizations, have not yet come to grips with how much the world has changed, nor with the possibilities, both beneficial and perilous, that result from living and leading in an era of super-transparency.

Our research aims to understand the causes of these changes, the nature of the new reality that results, and the implications for organizations and their leaders. In aggregate, the changes amount to a fundamental shift in what is commonly known and knowable that invalidate assumptions and practices we've often relied upon. Managers in all kinds of organizations need to understand this shift, how it changes the rules of all games they've been playing -- within competitive markets, in relationship with customers, within political contexts, and beyond.

From Data Puddles to Data Flood

Most people have long experience, from childhood, with puddles of water that form on the ground after a rainshower. Consequently, we are confident in our understanding of how puddles, and the water they contain, behave. We know, for example, that water can be moved between puddles, but that it does not move by itself. We can move water by dredging a channel between puddles or by using a container, a bucket or a cup, to move water from one puddle to another. We can even splash water from one to another, intentionally or not. Our most basic assumption about puddles of water echoes a law of physics: *water in a puddle tends to remain in that puddle, if no action intercedes to change that.*

There was a time not long ago when information behaved similarly. The goings-on in Argyll, Scotland, could be counted on to be known and paid attention to mainly by people in Argyll; information usually, but not always, remained within "information puddles." When information moved beyond a puddle, it was

because of deliberate action: Some identifiable person or organization moved it. If you wanted to be certain that information didn't move, you could build a barrier that kept the information contained (within an organization, say). Leaders have invested much over the years in building (fire)walls to keep information in place. And our assumptions about how information behaves still echoes -- to an inappropriate degree -- our understanding of puddles, also based on long experience since childhood that we gathered in an earlier age.

What, exactly, has changed? First and foremost, the *amount* of information. The volume of new digital data created every year is increasing exponentially. Individuals are the source of most of this data; seventy-five percent of all digital data is now created by consumers, the vast majority of it by handheld devices we carry around with us, smartphones.[1] Cisco, a company that knows a thing or two about data traffic, forecasts that mobile data movement will total 15.9 million terabytes (a million million megabytes) per month by 2018, growing at a 61 percent annual rate between now and then.[2]

Put simply, our information puddles have overflowed and become floods. Within a flood, water doesn't behave in ways that are easy to understand. It doesn't stay in place, and is difficult to contain. Flow in floods is governed by complex, often turbulent/chaotic local and non-linear physics. There still can be boundaries between reservoirs, but because ever-greater pressure builds behind them, they are more prone than ever to leak.

The emergence of personal, portable, digital data generation devices has been broad-based and astounding. Just about everyone has a smartphone in her or his possession, at all times. These not only generate huge volumes of new data, they're also endpoints for new channels of information flow that bypass intentionally constructed barriers. However much your company has invested in

firewalls, a quick photograph of key information displayed on a computer screen can be dispatched in a moment into the cloud, irretrievably, via means that, for the most part, work around your safeguards.

You can, of course, take steps to prevent this, with policies and technologies, but your degree of success will depend on your ability to imagine all the ways information might flow in a flood. In late 2014, when protestors in Hong Kong feared that cellular networks might be shut off, they started using FireChat, a smartphone app that connects mobile phones in a "mesh network," a phone-to-phone relay that routes information past shutdown cellphone towers.[3] Wander into a Brookstone in a U.S. airport, and ask them about their "pen with a secret"; that might *look* like a normal pen peeking out of some guy's shirt pocket, but it might actually be a video capture device which connects in two quick steps to the USB port on his computer -- where, again, it can be quickly dispatched to the cloud. Is that a smartpen someone is using to take notes in your meeting? If so, it's recording everything anyone says, and might be real-time uploading it to Evernote. And that other guy, is he wearing a smartwatch? If direct routes to the Internet are blocked, a person could just walk out with his pen, or watch, or a laptop he's downloaded to, or maybe a USB-stick, as Edward Snowden did when he carried 1.7 million classified documents out of one of the most secure organizations on Earth, the U.S. National Security Agency.[4] If you think your security procedures handle these risks, consider that ScanDisk has begun offering a 128 GB SD card smaller than your fingertip.[5] Maybe you think you've got that one covered too. But it's an arms race, and the cost of anyone of coming with a new information capture and transport option is just not that high.

Excitable Networks

The *New York Times* recently described how a message hastily composed and sent into the cloud by a communications executive, just before she got onto an 11-hour flight, destroyed her career by the time the plane landed.[6] People interpreted the tweet as racist (although, as the *Times* points out, it can be interpreted otherwise), and shared it via social media (Twitter), provoking a storm of criticism. By the time she restarted her smartphone after the flight, her employer had disavowed her. Similar examples are not hard to find: awkward jokes, out-of-context comments, captured and transmitted, can produce unexpectedly immense reactions as information finds its way out of an assumed information puddle and into the chaotic flood. We call this characteristic of information flow in a super-transparent world "amplification."

Amplification describes a tendency of certain images, stories, or other forms of information to resonate and splash especially widely. A precondition seems to be interconnectedness and overlapping networks of a certain density. The interactive nature of connections, the fact that posted information induces multifaceted reactions -- a provocative post on Facebook might draw others into an argument, for example -- causes information to feedback upon itself. More people are drawn in, not only by the original message, but also by reactions to it (and reactions to reactions).

But connections and interactions don't fully explain amplification. Certain events seem to have greater capacity to stir passions. An obvious injustice willfully committed, captured in a video and posted for the world to see, is a classic and recurrent motif within viral causes. As the NeverSeconds story illustrates, certain events incorporate compelling "plotlines." Plotlines can be

highlighted or brought into focus by the way events are presented or framed. In the early summer of 2013, a Reuter's photographer captured an image of woman, Ceyda Sungur, carrying a white bag and wearing a party dress at the very moment when she was pepper sprayed by Turkish riot police;[7] this "lady in red" photo became, as the web publication *The Verge* put it, "the symbol of Turkey's unrest" for reasons that seem largely aesthetic:

> With her stance relaxed and face downturned, Sungur, through Orsal's lens, is the epitome of passive resistance. The police officer's gas mask and crouched stance seem almost comically disproportionate to his target. With a barricade of shields framing the action with ominous uniformity, she stands alone and absorbs the spray.

The composition of this visual information, the way the photographer's craft frames and captures it, lends itself to amplification. This is a powerful form of artistry, akin to poetry or moviemaking.[8] Inexpensive but sophisticated tools for information capture and editing -- e.g., PhotoShop, iMovie -- now available to anyone, make it more likely that someone "out there" will be able to cast events that involve your organization in a surprising, passion-inciting plotline.

Agents of deliberate amplification work within the cloud. People with agendas reinforce and repeat items or interpretations of information. "Shamers" refuse to let a furor die down. When the earlier mentioned PR executive tried to start other jobs, shamers took to social media again, to spoil her efforts to move on. Even bystanders sometimes find themselves cast into plots that become amplified; a joke whispered privately to a colleague can be overheard and tweeted or posted by someone else.[9]

There's also positive potential in amplification. Sometimes enhanced transparency and amplification mean injustices, which would have remained hidden, get called out and punished. Sometimes the person or organization shamed deserves it, and there are no doubts about credibility of information. It's

likely that thuggish leaders now consider how things might look online before committing atrocities. Transparency is often a good thing; the word carries favorable connotations for this exact reason.

You might also think that "going viral" could be harnessed for marketing purposes. It can be, has been. Vipp, a company that sells high end kitchen and bathroom products, drove awareness of its iconic trash bins with a slick on-line video about making *haute couture* evening gowns for them to wear.[10] This was so incongruous or meaning redefining -- or something -- that many people shared it widely, to the company's great benefit.

But it's unsettlingly easy for marketers to underestimate or misjudge the chaotic behavior of flows within a flood. You can launch messages into the flood, but you cannot control where they will go or what others might do with them. Attempts to use social media for marketing can backfire. SodaStream, a company that sells a device for carbonating water at home, launched a social media campaign in 2013, describing its reusable bottles as socially responsible, only to find itself targeted by a viral campaign that shifted focus to complaints about one of its factories.[11]

Commodity Number Crunching

Definitions of "big data" vary, but the base idea is simple: easy, inexpensive access to large quantities of digital data combined with an ability to process it rapidly allows marketers, policy analysts, and others to conclude and/or predict things they could not in the past. Potential arises because new kinds of data have become routinely accessible, such as such geographic location linked to people and things. Additional potential arises because people now generate so much data as a byproduct of common behaviors, such as web searching and social

media posting. We can now predict flu outbreaks by detecting patterns in the symptoms people search for on Google, and marketers may know that your daughter is pregnant before you do (to cite two famous examples).[12]

One result of the ability to cheaply and rapidly crunch easily accessible numbers is a new degree of transparency. Cross referencing one data set with another -- "putting 2 and 2 together" -- allows number crunchers to discover things about you and your organization that you have not disclosed. Researchers have shown, for example, how supposedly anonymized data about customer purchases can be de-anonymized, by cross referencing.[13]

You might think this capability is limited to sophisticated analysts, but not so. Motivated individuals with modest skills and a moderately powerful computer can conclude a lot. Moreover, "the power of the crowd" enables ordinary people to accomplish sophisticated feats of transparency-producing analysis. In February 2009, a masked figure posted a video to YouTube that showed him abusing a cat. The video went viral, prompting collaborative detective work by cat sympathizers. The newly formed community cross-referenced the YouTube video with others, and with photos on Facebook, noting similarities in carpets, walls, and flags. Using a process worthy of crime scene investigators, they identified the masked figure and reported him to police. "Dusty the Cat" was rescued and his abuser cited for cruelty to animals.[14]

Security expert Dan Geer points out that individuals and organizations identify themselves in many ways.[15] Peoples' appearances can be identified at a distance with pattern recognition software, using a database available on social media, in the form of tagged photos. Even if *you* have not identified yourself in a photo on Facebook, odds are that someone else has. Your way of walking, detectable using the accelerometer in smartphones, identifies you. Your

heartbeat rhythm can too, as can your smell. Individuals and organizations produce a voluminous, mostly involutary, "digital exhaust," which reveals much more about them than they think it does.

Your Digital Exhaust Supercharged: The Internet of Things

The much-vaunted "Internet of Things" has already invaded our homes and businesses, not always securely. In a two-hour Internet scan[16], H. D. Moore of Rapid7 found 5,000 "wide-open" corporate boardrooms, equipped with misconfigured teleconference equipment[17]. Easily available tools can turn your home security system against you, and open your smart front-door lock. Your Skype-enabled TV can allow spying into your home.[18] An IP-enabled heating system tells people who know how to read it whether you're in or not – and let's not forget your car[19]. Our love affair with convenient technology may lead to an explosion of our digital exhaust, with streams of bundled, personal data sold on dark underbelly of the Internet. In our businesses and homes, proliferating network-connected devices make us more and more transparent.

Newly Formidable Cyber Snoopers

By now, everyone has probably heard of WikiLeaks, an organization committed to setting information free as a matter of first principle. The vast majority of emails previously stolen from Sony and recently released publicly by WikiLeaks contain no evidence of injustices that need addressing, but rather information in which people take mostly prurient interest -- rude things movie execs have said about movie stars, for example. No matter, pretty much all information needs to be free, according to some advocates.

The past few years have seen the rise to prominence of "hacktivists," entities like Anonymous that take up causes and use computer skills in ways that are sometimes borderline or outright illegal. In recent years, Anonymous has forced police organizations to reopen cases and companies to change ways of doing business, by bringing to light information they've obtained by unnamed means, and, sometimes, threatening to release the names and addresses of "guilty" insiders. People animated by a viral cause now often Tweet calls for help to Anonymous, much as the citizens of Gotham City sent the "Bat Signal" to the vigilante "Batman" in comics. Anonymous is not really an organization, because it has no stable membership, and temporary "members" are generally not known to each other, except by "screen names." Like many cause-motivated communities, Anonymous groups coalesce when "needed."

Anonymous has targeted many kinds of organizations, even hospitals, whose leaders took actions they did not like, often with impressive effect.[20] In 2010, for example, Anonymous took on HBGary, a firm that provided IT security consulting to the U.S. Defense Department and Intelligence Services. Aaron Barr, head of the company's Federal Division, attempted to infiltrate an Anonymous group that had shut down MasterCard and Visa computer systems (because these two firms had stopped processing donations to Wikileaks). But Barr made a mistake: he suggested in an interview with the *Financial Times* that he was closing in on his prey. Within 24 hours of the interview's publication, Anonymous took over the company's website, stole and deleted emails, and deleted the company's backup data; they even took over Barr's Twitter account, and erased the contents of his iPad.[21]

This group was eventually caught, and turned out not to be master criminals. Two were in their twenties (28 and 23), and three more were teenagers

(19, 19, and 16). They had access only to modest computers and tools, and had succeeded not only with online skills, but also by "social engineering" -- a low tech version of an old fashioned con, in which the perpetrators convince people inside the company to reveal information that they should not. The fundamental problem: so many of your information flows are available to people determined to access them, using tools and resources that, though effective, are not technically impressive. It's not difficult to hack your smartphone.[22] Cybercriminals, with more expertise and resources, add to this troubling mix, and unlike other forms of hackers, criminals don't brag about their exploits -- they keep them secret so they can use them again.

Growing Pressure for Openness

As organizations become inherently more transparent, government officials and policy makers simultaneously expect more disclosure, especially related to taxation, corruption, safety, and sustainability.[23] The financial crisis of 2008 gave rise to some of this, but monitoring inclinations of investigative journalists and NGOs, sometimes in league with previously mentioned cyber snoopers, are also contributing factors. Growing official expectations of transparency adds to the pressure that mounts behind information levies due to other causes.

Recommendations: Managing in a Super-Transparent World

Our research suggests several steps that managers can take take to adjust to the new super-transparent reality.

Examine assumptions about your ability to keep information contained -- You can no longer count on assumed information boundaries, either naturally occurring

or deliberately constructed. Systematically identify unrealistic assumptions, the points at which you might be unwisely assuming that you can contain information. You might be able to keep a few secrets, but it will be expensive and difficult. And there's always a risk it won't work.

Review your organization's strategy for vulnerability to unintended transparency -- To what extent does your strategy depend on containing information flows? Too much? Consider adopting business strategies that are not sensitive to unexpected information flows. Consider abandoning strategies that rely too much on your ability to keep secrets. Companies vary widely in the degree to which they compete based on keeping info private. Most organizations can successfully adjust their degree of strategy vulnerability.

Review your organization's operations for issues that might be a problem if revealed -- Review your supply chain. How many companies have been embarrassed in recent years by revelations about their operations in a developing country that also surprised leaders back at headquarters? Many firms now claim that their supply chain has become “unknowable” as a whole: except to an attacker with one particular mission. Consider hiring someone external to investigate your operations; fix problems you find, pre-emptively. Identify managers and management practices that might have problem potential; you're not witch hunting potential leakers here -- that's a losing game that itself risks becoming an online cause -- rather, you're looking for questionable behaviors or practices that might prompt leaking.

Develop a new PR approach that assumes others will put out information about your organization for their own reasons, and that you won't be able to get it taken down, or stop it from being rapidly communicated. -- The "Streisand Effect" describes what happened when the celebrity used lawyers to try to get an aerial photo of her house deleted from the web; every time they succeeded with one, ten more sprung up on other websites. When the prime minister of Turkey, tried to "rip out the roots" of Twitter, to prevent sharing of recorded phone conversations with his son, the tech community almost immediately created work arounds, and traffic on Twitter within Turkey increased.[24]

Managing your image has become a new game in a super-transparent world. It's more about influence than control, and it relies a lot on others. Being prepared to respond quickly, especially to information that is incorrect, is a big part of it. You won't be able to stop malicious falsehoods from ripping through social media. Some traditional media outlets, riding the sensation, may even try to avoid your corrections and keep a great plotline alive. But as you deposit accurate information into the cyberspace "record," providing responsible people with a basis for fact checking, you'll eventually put the brakes on irresponsible claims. Today most companies have nowhere near a fast enough response capability, however.

Take into account that new information flows change what people consider fair -- This one is subtle, perhaps least obvious but maybe most important: when information not previously accessible can suddenly be easily accessed, people often feel that it *should* be accessible. And when, as a result, information flows in new ways, interpretations of business activities change. One manager in a software company told us that discounts to prospective customers, which they

had long used in sales, became impossible once it became easy for existing customers to find out about them; indignant existing customers demanded similar discounts.

There's a parallel here to what happened to the music industry in the late 1990s, when the bits and bytes it owned -- the music in record companies' catalogues -- could suddenly flow easily across the Web. Considering themselves victims, record companies took legal action against downloaders -- only to discover that *they* had become the bad guys, in many people's eyes. Because their digital content *could* now flow so easily, many felt it was unreasonable to try to stop it. In the new information flow conditions, it suddenly seemed like extortion to force consumers pay $20 for a whole CD when they really wanted only one or two of the songs on it. The iTunes single song pricing model arose as a necessary response to customer's changed ideas about fairness.

Today's emerging super-transparent reality is like the music industry's late-90s problem writ large, and it will similarly force changes in the way a much broader set of companies operate. Now it's not just music flowing in surprising and uncontrollable ways -- it is the contents of our lives, captured by personal, portable digital data capture devices, mostly smartphones but also, increasingly, a wide range of other devices (smart pens, watches, wearables, etc.). And just as the music business never really recovered its old reality, so will we increasingly find our own realities, as individuals, organizations, and managers, permanently changed.

In a super-transparency world, it's important to be on the look out for shifts in what your customers and the public consider reasonable. You won't anticipate them all. Expect to be caught wrong-footed when customers or the public suddenly see something that your organization does in a surprisingly

different light. The shift in interpretations of what you do as a manager, and of how your organization behaves, will require that you to make changes. Even if you can't be ready for the all the challenges, you'll be better off beginning to think about this now.

---

[1] https://www.mobilecause.com/mobile-data-traffic-for-charities/. The number of smartphones now exceeds the world population.

[2] Cisco Visual Networking Index, see http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html.

[3] N. Cohen, "Hong Kong Protests Propel a Phone-to-Phone App," *New York* Times, October 5, 2014, http://www.nytimes.com/2014/10/06/technology/hong-kong-protests-propel-a-phone-to-phone-app-.html

[4] L. Franceschi-Bichhierai, "Snowden Stole Secret NSA Documents with a Flash Drive," *Mashable*, June 13, 2013. http://mashable.com/2013/06/13/snowden-nsa-thumb-drive/

[5] A. Cunningham, "SanDisk's 128GB microSD card is the biggest, tiniest storage you can buy," *Ars Technica,* February 25, 2014, http://arstechnica.com/gadgets/2014/02/sandisks-128gb-microsd-card-is-the-biggest-tiniest-storage-you-can-buy/

[6] J. Ronson, "How One Stupid Tweet Ruined Justine Sacco's Life," *New York Times*, February 12, 2015, http://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html

[7] A. Toor, "How a Lady in Red Became the Symbol of Turkey's Unrest," *The Verge*, June 7, 2013, http://www.theverge.com/2013/6/7/4405412/ceyda-sungur-lady-in-red-photo-becomes-symbol-of-turkey-protests

[8] See L. Devin and R. D. Austin, *The Soul of Design*, Stanford University Press, 2012.

[9] J. Ronson.

[10] See vipp.com.

[11] L. Abramson, "SodaStream Criticized for West Bank Plant," *NPR*, February 4, 2013, http://www.npr.org/2013/02/04/171033498/sodastream-criticized-for-west-bank-plant.

[12] B.E. Hernandez, "Google Knows Where the Flu Outbreaks Are," *NBC,* January 10, 2013, http://www.nbcbayarea.com/blogs/press-here/Google-Predicts-Flu-Trends-186344082.html; K. Hill, "How Target Figure Out How a Teen Girl Was Pregnant Before Her Father Did," *Forbes,* February 16, 2012, http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

[13] J. Bohannon, "Credit Card Study Blows Holes in Anonymity," *Science,* January 30, 2015: Vol. 347 no. 6221 pp. 468.

[14] http://knowyourmeme.com/memes/events/kenny-glenn-case-dusty-the-cat

[15] https://youtu.be/hxLJExWk9GE (video) or http://geer.tinho.net/geer.rsa.28ii14.txt (text).

[16] R. Vamosi, "Corporate Video Conference Systems Fail Secure Implementation," *SecurityWeek,* January 26, 2012, http://www.securityweek.com/corporate-video-conferencing-systems-fail-secure-implementation

[17] M. Smith, "Hacks to Turn your Wireless IP Serveillance Cameras Against You," *NetworkWorld*, April 14, 2013, http://www.networkworld.com/article/2224469/microsoft-subnet/hacks-to-turn-your-wireless-ip-surveillance-cameras-against-you.html

[18] "Paul," "Security Hole in Samsung Smart TVs Could Allow Remote Spying," *The Security Ledger*, December 12, 2012, https://securityledger.com/2012/12/security-hole-in-samsung-smart-tvs-could-allow-remote-spying/

[19] H. Kelly, "The Five Scariest Hacks We Saw Last Week," *CNN*, August 5, 2013, http://edition.cnn.com/2013/08/05/tech/mobile/five-hacks/

[20] M. B. Farrell and P. Wen, "Hacker Group Anonymous Targets Childrens Hospital," *Boston Globe*, April 24, 2014.

[21] P. Bright, "Anonymous speaks: the inside story of the HB Gary hack," *Ars Technica,* February 16, 2011, http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/.

[22] T. Parker, "Researchers Demo 92% Success Rate in Hacking Smartphone Apps," http://www.fiercewireless.com/tech/story/researchers-demo-92-success-rate-hacking-smartphone-apps/2014-08-24

[23] See "The Openness Revolution," *The Economist*, December 13, 2014.

[24] C. Letsch (March 21, 2014). "Turkey Twitter users flout Erdogan ban on micro-blogging site". The Guardian. Retrieved, December 3, 2014.