Chapter 3

The Gates Come Down

A peculiar silence reigned in most major newspapers and TV networks the first few days after Trent Lott, celebrating fellow Republican Senator Strom Thurmond's 100th birthday in late 2002, seemed to wax nostalgic for a racist past. Lott, then majority leader of the U.S. Senate, recalled Thurmond's presidential campaign in 1948, a race in which he called for the preservation of segregation. The nation would be better off if Thurmond had won, Lott said.

It was an outrageous assertion, but barely noticed at the outset. ABC News mentioned it. *The Washington Post* had a story but buried it. And that was about all we heard from the major media. But the silence didn't last, because Lott got a taste of tomorrow's media: the swarm of webloggers, emailers, and other online journalists who are changing some long-established rules.

The flow of outrage and information was complex.[66] But the bottom line was that webloggers and other online commentators, far more than mainstream journalists, kept the story of Lott's remarks alive despite the major media's early disinterest. Liberal bloggers, such as Joshua Marshall on Talking Points Memo,[67] were early to sound off, but several conservatives also chimed in. In some cases, bloggers were almost as outraged by Big Media's inattention as by the senator's statements and initially weasely expression of regret for his remarks.

A few days later, the story that didn't go away was running, full-bore, in the national media. Even President Bush was obliged to denounce Lott, a key congressional ally. In the end, no one was surprised when Lott, under enormous pressure, resigned as majority leader.

While bloggers could not have brought down Lott on their own had Big Media not taken up the story, the Lott debacle was, by all accounts, a watershed. Weblogs claimed "their first scalp," said card-carrying establishment conservative John Podhoretz in his *New York Post* column.

Call them newsmakers. Call them sources. Call them the subjects—and sometimes, in their view, the unwilling victims—of journalism. But however we describe them, we all must recognize that the rules for newsmakers, not just journalists, have changed, thanks to everyone's ability to make the news.

Most of today's politicians and business people, and virtually all powerful institutions, accumulated their status and authority in a different era. They see the news media's traditional hierarchies reflecting their own centralized, top-down model, with distinct control points. In this model, public relations and marketing departments deal with the press and the public. Executives deal with reporters when necessary. News is controlled from within the organization and managed when outside forces intervene.

It's an industrial age model: manufacturing news. It still works, to some degree, but it's less and less effective. If markets are conversations, as the *Cluetrain Manifesto* authors have noted, then journalism—the information people need to manage their lives—will increasingly be part of those conversations.

Newsmakers need to understand that the swirling eddies of news are not tiny pools on the shoreline. Information is an ocean, and newsmakers can no longer control the tide as easily as they once did.

So they must face at least three new rules of public life.

First, outsiders of all kinds can probe more deeply into newsmakers' businesses and affairs. They can disseminate what they learn more widely and more quickly. And it's never been easier to organize like-minded people to support, or denounce, a person or cause. The communications-enabled grassroots is a formidable truth squad.

Second, insiders are part of the conversation. Information no longer leaks. It gushes, through firewalls and other barriers, via instant messages, emails, and phone calls.

Third, what gushes forth can take on a life of its own, even if it's not true.

SPREADING THE WORD

As noted earlier, modern communications have become history's greatest soapbox, gossip factory, and, in a very real sense, spreader of genuine news. At one time, an individual with an issue had few options. He could stand on the corner and rant, or post a sign, or write a newsletter, or pen a letter to the editor. Today, if his argument is sufficiently moving and/or backed up with facts, the tools at his disposal can make it a global phenomenon. The autonomous linking machine—consisting of people who care enough to spread the word, plus new tools such as RSS, which widely disseminate what they write—launches into action. And how the word does spread.

Even before the Web rose to prominence, the online world was making companies pay attention. In 1994, Usenet, the system of Internet discussion groups, helped teach a lesson to Intel, which makes most of the processors that are the central brains of personal computers. News of the "Pentium bug," a math-calculation flaw in a version of the Pentium processor, first spread via Usenet before it was picked up in the popular press. At great expense financially and to its reputation, Intel had to replace many of the flawed chips. "Our immediate lesson was from that moment onwards, you cannot ignore that medium [the Internet] and that that medium was going to get more and more important at setting opinions," an Intel executive told the CNET news service in 1999.[68]

A decade after the Intel debacle came another relatively trivial, but still revealing, example. In early 2004, with great fanfare, including a Super Bowl commercial, Pepsi announced a "free songs" promotion. Buyers of Pepsi could look at the underside of the bottle cap and, about one out of three times, win a free song download from the Apple iTunes music web site. But someone noticed a flaw in the bottle design. He or she figured out how to tilt the unopened bottle just so and discover whether the bottle contained the code for the song. Once upon a time that information would have remained within a small community of people, but in the Internet age, that information was almost instantly available to anyone with an Internet connection in the form of a document titled "How to never lose Pepsi's iTunes giveaway."[69] And there was nothing Pepsi could do about it. If someone knows something in one place, everyone who cares about that something will know it soon enough.

Consider a far more profound example, a case with true life-or-death implications: the SARS epidemic that began in the Chinese province of Guangdong in November 2002. The repressive government, accustomed to controlling the news, at first didn't allow the medical community to tell anyone what was happening. But in early February 2003, the news began to leak out anyway, not through newspapers or television or official announcements, but through SMS, or short messaging through mobile phones, a modern form of word-of-mouth. And the word was grim: people were sick and in some cases dying from a particularly virulent form of pneumonia. That led to some news coverage, probably much earlier than might have happened had the people not literally taken news delivery into their own hands.[70]

Once SARS became a household word and panic began to set in, SMS became a medium of choice for the government, too.

Hong Kong authorities used it to attempt, not very successfully, to dampen unfounded rumors that were spreading on the Internet.[71]

Now add "moblogging" and its kin to the equation—the use of camera-equipped mobile devices by just about everyone, in a world where we must assume that people are constantly taking pictures in public places.

Newsmakers, especially Hollywood stars and other celebrities, already loathe the "paparazzi" photographers who follow them around and snap pictures in unguarded moments. What will happen when 10 average citizens aim their phones at the stars and zap the images they take to their friends or to web sites? Still images are only the beginning; video cameras will become part of our phones soon enough. The paparazzi have better cameras and are better picture-takers, but the swarms of amateur paparazzi will satisfy most of the public's insatiable hunger for news about their favorite celebrities. And for the people who live in the public eye, that eye will never blink when they're outside of their homes.

That, of course, is a relatively trivial example of what's coming. Camera phones and other carry-everywhere photographic and video devices may give people powerful tools to prevent crime; as CNN reported in 2003, a 15-year-old boy snapped a camera-phone picture of a would-be abductor, helping the police find the man.[72] These devices will also greatly accelerate the way we document history.

As of early May 2004, it was still unclear who took the digital photographs of Americans abusing Iraqi prisoners in Abu Ghraib prison, but their escape into the public sphere was already seen as a negative pivot point not just in the conflict but in the world's view of America. Even if the military and the Bush administration had wanted to keep the near-torture covered up, once the photos had been taken and started to make their way around, their wider distribution was almost inevitable.

We are a society of voyeurs and exhibitionists. We can argue whether this is benign or repugnant, but when secrets become far more difficult to keep, something fundamental will have changed. Imagine Rodney King and Abu Ghraib times a million. Police everywhere must already wonder if they are being taped. Soon they will have to assume they're being caught on digital video. This has obvious benefits, such as curbing police misconduct. But everyone who works, or moves around, in a public place should consider whether they like the idea of all their movements being recorded by nosy neighbors. We may not be able to choose between the benefits of ubiquitous cameras and their drawbacks.

It's worth reflecting how events of the past would have looked had tomorrow's technology been available at the time. Let's apply that to the horrific events of September 11, 2001. Our memories of that awful day stem largely from television: videos of airplanes slamming into the World Trade Center, the fireballs that erupted, people falling and jumping from the towers, the crumbling to earth of the structures. Individuals with video cameras captured parts of this story, and their work ended up on network TV as well. The big networks stopped showing most graphic videos fairly quickly. But those pictures are still on the Net for anyone who wants to see them.

We also learned, second-hand, that people in the airplanes and Trade Center towers phoned loved ones and colleagues that awful day. What would we remember if the people on the airplanes and in those buildings all had camera-phones? What if they'd been sending images and audio from the epicenter of the terrorists' airborne arsenal, and from inside the towers that became coffins for so many? I don't mean to be ghoulish, but I do suggest that our memories would be considerably different had images and sounds of that kind ricocheted around the globe.

TRUTH SQUAD

In September 2002, Microsoft posted a semi-bogus web page advertisement featuring a winsome young woman, identified as a freelance writer, who'd supposedly switched from a Mac to a PC. The page was entitled "Mac to PC: Mission Accomplished, Convert Thrilled," and was a response to Apple's "Switch" (from PCs to Macs) campaign. A commenter on the Slashdot site[73] discovered and reported that the picture of this supposed freelancer was from a Getty Images archive.[74] The Associated Press's Ted Bridis then scoped out the rest of the story, which was, of course, not the one Microsoft had been floating. A Microsoft PR man, weaving around some direct questions from me, said: "It was a mistake that it was posted, and Microsoft took it down as soon as it came to the attention of the Windows XP marketing team. Microsoft regrets any confusion it may have caused."

I suggested at the time that people might be making too much of the half-fake nature of the ad. After all, the people who pitch products in TV and print advertisements are usually actors. But when Apple's PC-to-Mac converts were apparently all real, including their pictures, Microsoft's phoniness was all the more obnoxious.

What made the incident stand out was the way the untruth unraveled. Slashdot's readers, members of a powerful online community, got on the case. They were the first to show that something wasn't kosher with the Microsoft page. And they deserved much of the credit for the story coming out in the first place.

The accumulation of data is a powerful research tool for anyone who wants to drill deeper into an issue. The earnest pamphleteer can now do more than challenge something. He can build an online encyclopedia of detailed information on any topic and keep expanding it—a vibrant archive and organizing tool that others use and augment. Combined, this becomes an impossible-to-ignore force.

And it's been happening for some time. In the mid-1990s, McDonald's Corp. faced some angry online citizens and never quite figured out what to do about them. The fast-food behemoth took two activists to court in London, arguing that the company had been libeled by their pamphlets. The activists counter-sued, and then created the path-breaking "McSpotlight" web site[75] to support their side in what became the longest-running such court case in British history—a trial that became a referendum on the McDonald's empire and its sometimes unseemly actions around the world.

One of the most useful aspects of McSpotlight was its brilliant deconstruction of McDonald's marketing materials. Using web frames, an online display technique, the site showed McDonald's public-relations message on one side of the screen. The McSpotlight rebuttals appeared on the other side.

McDonald's officially won the trial, or at least a portion, in part because British libel laws are tilted toward plaintiffs. The company was trying to extract money from a stone, however, so after its enormous legal bills, it had lost a serious financial battle. And, crucially, the company took a beating in the court of public opinion. The McSpotlight court case and web site revealed a multinational giant that, at the very least, had an occasional deficit in ethics. More people knew about that record after the trial than before.

McSpotlight didn't fold with the end of the trial. It expanded its mission even as the trial was proceeding to include a wider look not just at McDonald's, but multinational corporate behavior.

The tobacco companies, another widely criticized multinational industry, also felt the weight of web-based documentation in the mid-1990s when the University of California, San Francisco created the Tobacco Control Archives, an assortment of documents that antismoking forces have found valuable in their war against the industry.[76] Stanton Glantz, a UC San Francisco professor who's been studying the tobacco industry and its contributions to political candidates, said the university's librarians solved several problems by posting the material on the Web, thus getting the material to people who wanted it while saving time for university personnel. Only later did the power of the new medium become clear, he said, when antismoking forces elsewhere started using the material in their own campaigns.

The Web is "a very important development," he told me in 1996, not long after he'd created the archive. "It allows people like me—kind of detail nerds—to make the resources available, fairly inexpensively and in however much depth we want."

And it's allowed more and more activists to shine a light on material that powerful institutions would prefer to hide. Government officials are as secretive as companies, perhaps more so. Which is why we should thank people such as Russ Kirk for his Memory Hole site,[77] a growing archive of important material. The site's home page declares its mission is "rescuing knowledge, freeing information." It achieves its goal brilliantly. In a journalistic coup, Kirk put Big Media to shame in April 2004 by using the Freedom of Information Act to get the military's photos of America's Iraq war dead—the moving and dignified pictures of flag-draped caskets that other media hadn't thought to request.

The repositories continue to expand, and they're moving an information imbalance closer to equilibrium for everyday citizens, not just for activists and scholars. In his 1914 book *Drift and Mastery*,[78] Walter Lippmann warned that civilization was becoming so complex that "the purchaser can't pit himself against the producer, for he lacks knowledge and power to make the bargain a fair one." The knowledge equation has unquestionably shifted back towards the purchaser, and the power is following. Users of appliances and devices, whose inner workings were once trade secrets and inaccessible to consumers, have been tapping that power.

A couple of years ago, I wanted to upgrade the hard disk on a video recorder I use at home. It was a DishPlayer, attached to my Dish Network satellite system. The original drive held 17 gigabytes, storing roughly 12 hours of video, and a new 40 gigabytes drive was on sale at the local electronics store for about $120. Unsurprisingly, Dish Networks wasn't especially interested in telling me how to do it. And there were no traditional sources either, such as printed hobbyist magazines devoted to upgrading DishPlayer recorders, or newsletters that explained how to fire up the various diagnostic modes using the remote. The Web—and discussion groups in particular—was my go-to source. I found solid instructions online,[79] gave them a try, and, voila, I had a 30-hour storage system. (I also found instructions on other bulletin boards where users had posted warnings to avoid instructions that hadn't worked for some users—advice I took; the instructions I ultimately followed came with a warning that the upgrade might fail if I wasn't careful, but others posting to the board agreed the fix would work if done properly.)

What I did was minor-league tinkering compared with what others are doing every day. The hacking phenomenon—and I use the word "hacking" in its most benevolent sense—has expanded into the world of gadgets and everyday tools. People who want to improve what they've bought are studying how things work, whether the products are traditional electronics or things with a software component, and these customers are making adjustments—hacks, as they're known—that either make the products better or change their nature entirely. And they're doing it by informing each other, in an open source manner that brings the community's best minds to bear on common problems.

In early May 2003, Apple Computer released a new series of iPod handheld music players. It took no time for the iPod mavens to run tests and discover functions that Apple hadn't mentioned in its product literature. "Well," a report began on the iPoding site,[80] "we couldn't wait so we went to the local Best Buy and picked up a new Gen 2 15 GB. It's going to be taken apart soon, but we first ran Diagnostic Mode on it. It has a recording feature! There is also a test for LINEIN that does recording too."

As a journalist who frequently uses a digital recorder for interviews, this was interesting news for me. But the point was that it was news, period, and it was broken by the people who used the device most ardently, not by the company that made it. Apple may have thought it was keeping future plans to itself (though that's debatable), but it couldn't keep smart people from figuring things out for themselves or from broadcasting what they discovered.

The process has something in common with the car-defect reports that eventually make their way back to manufacturers. In the old days, we'd learn of those defects if we encountered one, if the manufacturer told us, if the defect was sufficiently major to warrant news coverage, or if the government ordered a recall. Now we learn about them from user groups and from the Internet.

One of the more notable examples of learning about unauthorized things over the Internet has been the tinkering of automobile electronic systems, a trend automakers universally dislike. Earlier auto enthusiasts tinkered with carburetors and manifolds; now they tinker with software code. "Much to the chagrin of the automobile manufacturers and in spite of tight security, computer hackers have been able to reverse-engineer the code for most engine controllers within just a few months of the code's appearance," wrote Warren Webb, technical editor of EDN Access, a trade magazine.[81] "By adjusting the control-system parameters, hackers can defeat the California-emissions controls and increase automobile performance." And people doing the hacking tell others what they've done. A quick web search will turn up dozens of sites where people share their knowledge of various tweaks, such as how to boost horsepower.[82]

Now the automakers have a legitimate concern, especially if the hackers disable smog-control systems or introduce some behavior that might make the car unsafe. For the most part, however, the people doing the hacking are learning ways to make car engines and other systems more efficient and reliable. Banning such information sharing—sometimes through the use of obnoxious copyright lawsuits—is tantamount to giving manufacturers unprecedented control over customers. Which, of course, is something they want to have—but they are risking more than just customer unhappiness if they push the control too far. They are risking their businesses.

Eric Von Hippel, business professor at the Massachusetts Institute of Technology, thinks businesses should encourage some level of hacker behavior, not shun it.[83] He told me companies should be doing everything they can to support and encourage the "lead users"—people like me with my Dish-Player—to find flaws in products and improve them. Just as journalists should not be threatened by a more knowledgeable audience, companies should not be threatened by smart customers who care enough to make products better. When your customers offer their expert assistance, the smart move is to say Thanks.

LOOKING DEEPER

If customers exchanging information wasn't a big enough change, consider the new category of self-organized customer information erupting around us.

In his research labs, University of Tokyo Professor Ken Sakamura has been experimenting with tiny chips that contain short-range radios, embedding them in various products and other items. In his Ubiquitous Networking Laboratory,[84] he scans them and links the product identification to a database with much more information, including the product's history. Someday, he told me, everything will have these ID tags, and we'll be able to get vast amounts of information about what we touch and buy. For example, a head of lettuce could tell us where it was grown and whether the farmer used pesticides. Or a bottle of pills could tell us whether the drug would pose risks if taken with another drug we've been prescribed.

Marc Smith, a Microsoft researcher,[85] has offered another glimpse of the future with his "Aura" system. Using what is essentially off-the-shelf technology, he's equipped a handheld computer with a wireless Internet connection and a bar-code scanner that he uses to scan products in stores. His computer then connects to a server that collects data from Google and other sources, and shows him the results on the handheld screen.

Suddenly, far more than the price is available. Data about the product, and its maker, is available in a far wider information ecosystem. Was a shirt made by slave labor? Did the can of processed food come from a company with a record of poisoning streams in its factories' backyards? Did the company have a reputation for being good to employees and the environment? Smith likes to show a supermarket scan he once did of a cereal box. The top item in Google reveals that the maker had at one point recalled the product because a significant ingredient wasn't on the label. That might be interesting information to someone hyper-allergic to that ingredient. If every object can tell a story, Smith said, "One of the more profound stories is 'If you eat me I will kill you.'"

Now add location to this notion. During the SARS crisis of 2003, a Hong Kong mobile phone company created a system to alert people if there had been any cases of SARS in the building they were about to enter. They used publicly available data and combined it with location-based software in the phones.[86]

It all suggests a higher level of transparency, not granted willingly by the "newsmaker"—a government or corporation—but captured by the user. It's possible because all kinds of data and metadata (information about information) is now escaping into the wild. The downsides are plain, including the consequences of erroneous information and potential invasions of privacy. But the positive uses are also evident.

BUBBLE, BUBBLE, TOUT AND TROUBLE

The name Jonathan Lebed doesn't mean much to people anymore, but it should hang on the wall of every corporate public-relations executive's office. Lebed was a stock market player, one of many in the bubble days of the late 1990s whose recommendations of shares online helped fuel price rises before the crash. He was hardly alone in manipulating the market. Famous analysts on Wall Street issued absurd recommendations to buy stocks—including some they considered dogs privately—that then plummeted. Lebed didn't travel in such elevated circles. He was a New Jersey teenager who, under false names in Internet chat rooms, made hundreds of thousands of dollars by touting various shares. He ended up settling with securities regulators, who allowed him to keep much of his loot. As Michael Lewis noted in *The New York Times Magazine*, it was never really clear whether he was doing something flat-out illegal or just ethically questionable.[87]

Companies should remember is that this kind of activity—and much worse ways of playing the system—hasn't gone away. It's still rampant.

But it's part of a wider phenomenon: the ability of anyone to join in a global dissection of corporate behavior and finances. The problem for the average person entering this cyberworld, as I discuss at greater length in Chapter 9, is distinguishing between truth and falsehood. The problem for the subject of the discussion—the newsmaker—is bigger.

For honorable public companies, some of the worst dilemmas arise in forums where people discuss stock prices and corporate financial performance. The urge to boost the value of one's own portfolio, or to spread information that helps depress the price and make short-selling more lucrative, is too obvious to ignore. But even in these forums you can find nuggets of useful information. Journalists who cover companies and fail to monitor such places are guaranteed to miss relevant data.

Companies should monitor these discussions carefully, of course, even when there's no obvious participation by corporate officials. Most do, and for the same reasons the journalists watch the discussions—to learn something—but also to see if people are spreading misinformation or worse.

Almost everyone on these systems uses a pseudonym. Sometimes it's insiders who are doing the posting. At least insiders posted more frequently before companies started going to court to get the names and addresses of—depending on one's view—whistle blowers or revealers of trade secrets and other confidential information. Sometimes postings become a target of corporate lawyers, as we'll discuss in Chapter 10. But courts are beginning to tell companies they can't require the identification of anonymous chat-room posters unless there's some actual evidence of libel.

Companies should ponder a more interesting question than whether they should chase down and respond to every rumor they see online. What if, instead, trade secrets are simply a vestige of a dying era? With few exceptions, I'd suggest that the more transparent a company is, the more likely it will succeed in a networked world. I wouldn't take this so far as to say companies should bare all; that's obviously absurd. But Doc Searls's shot at the Segway, inventor Dean Kamen's two-wheel scooter that won so much publicity when it emerged from a massive rumor mill, was well-deserved. Searls, not coincidentally a *Cluetrain Manifesto* coauthor, wrote on his blog[88] in December 2001:

> I believe that Dean Kamen's creation is so original, and his vision so personal, that there is no way anybody else could have cloned it or stolen its thunder before it came out. So it annoys me that he and his crew were so deeply secretive about the thing, even though I know secrecy is pro forma in the invention business.
>
> But did it do any good?
>
> Yes, there was some nice buzz about "Ginger" (aka "IT") when it was in development, [but] there wasn't much to talk about. And now that it's out, there still isn't. We don't know enough. We haven't been talking about it.
>
> If Kamen and crew kept no secrets about Ginger when she was in development, I'd betcha there would now be far more demand, and far more creative thinking about what could be done with it.

> And I'll guarantee you this: the most original uses for this original machine will be ones Kamen didn't imagine when he created it.

This is heresy for many, but it's going to be more and more obvious as time passes. Maybe the discussion boards, far from being a threat, are a boon. Of course, they'd be even better if companies participated officially. In fact, the best examples are support forums hosted by the sellers of products in which designated staff members participate and postings are not censored, except in cases of obvious libel or deeply offensive language. One company that has grasped this fairly well is EchoStar, which makes the home satellite TV system I use. A spokesman told me the company's technical people participate indirectly in the online news chatter, letting webmasters know when there's misinformation on their sites. In effect, Dish Networks winks at the users' activity but tries to prevent people from causing real damage.

In an article explaining the surprising showing by Howard Dean in the early stages of the 2004 presidential campaign, Ed Cone, a journalist in North Carolina, made some telling observations that apply far more widely:

> Television, radio, print and mail can create awareness and desire for a product. Senders control the presentation and, if intelligently worded and presented, the messages cause an individual or company to vote with its dollars, by buying the product. But the lesson of Dean's campaign is that the Web is not for micromanagers. With the Internet, an effective campaign creates a community that will on its own begin to market your product for you. Properly done, you won't be able—or want—to control it.[89]

SWARMING INVESTIGATORS AND SPIES

In breaking down barriers and secrecy, our weapons have several edges. In his important book, *The Transparent Society*,[90] David Brin suggested that privacy is becoming a relic of a pre-technological time. Preserving old-fashioned privacy was impossible, he said, because modern technology would overwhelm us with its snooping power and the collection of vast amounts of data. Our only recourse, he suggested, was to turn the same tools back on the watchers, to create what would amount to a détente in which we all reserved some dignity. I don't believe it will happen this way because governments and large organizations will never permit citizens to have the same access to their inner sanctums and methods that they insist on having to our personal and professional lives.

Even so, regular people are beginning to discover ways to redress the balance. Witness the case of former U.S. National Security Advisor John Poindexter, who helped dream up the grotesquely invasive "Total Information Awareness" program. Thanks to new technologies, he got a taste for himself.

Total Information Awareness, you may recall, was the Bush administration's data-mining program, designed to ferret out suspicious activities by potential terrorists. It would gather vast amounts of data on individuals by collecting and linking records from financial, driving, criminal, court, medical, and other databases. Poindexter, the former rear admiral and Iran-Contra scandal figure from the 1990s, was in charge of putting this program together.

Civil libertarians picked up and amplified a column by Matt Smith from the December 3, 2002 *San Francisco Weekly*, an alternative newspaper.[91] The column, wrote Net activist John Gilmore, "points out that there may be some information that John M. and Linda Poindexter of 10 Barrington Fare, Rockville, MD, 20850, may be missing in their pursuit of total information awareness. He suggests that people with information to offer should phone +1 301 424 6613 to speak with that corrupt official and his wife. Neighbors Thomas E. Maxwell, 67, at 8 Barringon Fare (+1 301 251 1326), James F. Galvin, 56, at 12 (+1 301 424 0089), and Sherrill V. Stant (nee Knight) at 6, may also lack some information that would be valuable to them in making decisions—decisions that could affect the basic civil rights of every American."

Gilmore took it a step further. He downloaded publicly available satellite photos of Poindexter's neighborhood and posted them on the widely followed Cryptome web site.[92] He also urged people with access to databases containing information on Poindexter and other privacy invaders to expose it as an example of what would go wrong with Total Information Awareness.

A few days later, privacy activist Richard Smith chimed in on the Cryptome site. "It looks like members of the Total Information Awareness (TIA) development team at DARPA don't like the lime-light. All of their bio's [sic] were removed from the Information Awareness Office[93] Web site sometime during the past couple of weeks. However the Google cache still had all of the bio's cached, so I have put copies on my Web site." He listed the web address.

Was this Total Information Access, judo-style? Not entirely. The program was officially put out to pasture, but the snoops are still trying to make it happen via other means, and they'll always have much more data than their opponents. But in the future, they will understand that looking over shoulders is no longer the sole province of the spies. In this case, the swarm of activists and commentators, who individually could make scarcely a dent, was collectively making itself heard.

WATCHING JOURNALISTS

What industry is traditionally among the least transparent? Journalism. We have been a black box, and have become only slightly more transparent in recent years. But the public is demanding more transparency in our own field, and is doing some reporting of its own when we fail to respond in satisfying ways.

Jim Romenesko's Poynter Institute media blog,[94] the first and still the best of its genre, has become a water cooler not just for journalists but for people who observe journalism. Generally, the blogging community is not shy to go after newspapers, magazines, and broadcasters for real and imagined offenses against fairness and accuracy. For journalists, who are among the most thin-skinned people around, this trend has been something of a shock. We are not accustomed to being scrutinized the way we scrutinize others, however healthy it is that we are.

Even *The New York Times* was forced to pull down its veil in 2003, when the infamous Jayson Blair's journalistic cons become one of the newspaper's worst scandals. The *Times*' appropriately scathing internal analysis of the mess, the "Siegel Report,"[95] revealed a horror show of missed communications and lax management on top of plainly corrupt behavior by Blair himself. But the Siegel Report appeared briefly online and then disappeared, prompting Jay Rosen at New York University to ask what had happened to it. Eventually, and in large part because of Rosen's prodding, the document reappeared online.

In early 2004, amid political reporting that many in the blogosphere found wanting, a suggestion emerged to improve journalism in general. The idea was to follow individual reporters' political coverage on web sites, relentlessly tracking errors and omissions and exposing them to the world. I commented in my own blog, and on Rosen's PressThink site, where the notion first got some traction:

> I like the idea that people are watching what I say and correcting me if I get things wrong—or challenging my conclusions, based on the same facts (or facts I hadn't known about when I wrote the piece.) This is a piece of tomorrow's journalism, and we in the business should welcome the feedback and assistance that, if we do it right, becomes part of a larger conversation.
>
> But if the idea is to create some kind of organized collection of Truth Squads, I'm less comfortable. Here are just three of the many, many questions/issues that come immediately to

mind (and as you'll see, I'm not alone in wondering these things):

1) Who's doing the watching? A self-appointed "watcher" is an antagonist in most cases, convinced before he/she starts posting criticisms that the journalist in question is getting things wrong, whether due to incompetence or animosity. Journalists confronted with this kind of attitude don't respond well, and probably won't respond at all.

Paul Krugman has a cadre of online critics who make my own look benign. Occasionally they make a sound point. Much of what they say is incorrect. And some of it is debaters' tricks: using straw men to shoot down things he didn't say, or saying something that may be true but is off point, etc.

2) Will journalists who do participate in the online discussion of their work—and many will be forbidden to do so by their organizations, probably for legal reasons—hit the law of diminishing returns?

I recall the quasi-religious debates over the OS/2 operating system back in the early and middle 1990s. I was a fan of OS/2 but not sufficiently infused with the religion. Once in a while I'd post a note in a Usenet discussion where something I'd written was either being misinterpreted or had been seriously twisted. I'd then get hammered by one of the more fervent OS/2 acolytes who'd deconstruct every sentence and ask further questions, few of which were actually relevant (in my view) to the issue. I quickly learned that I had time for correcting outright mistruths and not much else. (I also had defenders in the newsgroup, which helped.)

3) Why should anyone trust what critics say any more than what the journalist says? An assertion that a journalist has a fact wrong is not, in itself, true. It's just an assertion.

Do we need Truth Squads watching the Truth Squads? There are, amazingly, sites that deconstruct the anti-Krugman stuff. But you'll forgive a casual reader for ignoring almost all of it.

None of these issues means that Web watchers are a bad idea. But if the idea is to really make journalism better, I'm just not convinced this will work.

This prompted Donald Luskin, an investment officer and a prominent Krugman debunker who writes an entertaining and frequently instructive economics and policy blog[96] to write: “Wouldn’t it be nice for journalists like Dan Gillmor if everyone who disagreed with their pronouncements just sent friendly little emails and let them decide how and whether to respond? How unseemly that, instead, some of us have become ‘organized Truth Squads.’ Apparently only Big Media has the right to be organized.”

I responded on mine:

> First, I welcome comments on this blog, and have had some lively debates with some fairly angry critics here from time to time; Luskin could have posted a copy of his remark right on this page, but that would have contradicted the implication that the only good feedback is happy-face e-mail. (Note that Luskin doesn’t allow people to post comments directly, and seems to prefer more of an echo chamber than actual debate in the letters he does post.) Second, I’ve been arguing for some time that the little guy needs to get active and organized to have a chance against Big Everything (including Big Media). Luskin either doesn’t know that or doesn’t care, and somehow I’m not surprised.

I’m having some second thoughts about the comments feature, for many reasons that I’ll discuss in Chapter 9. But this much is clear: the trend toward media transparency is inevitable, and it will engender debates that help users of journalism understand a process that has been hidden from view. Will we ever be entirely transparent? Not likely. But we can’t avoid—and shouldn’t try to avoid—more openness.

TURNING THE TABLES

We've seen how modern communications give anyone who cares the tools to learn more—far more—about people and organizations that in the past tried to ration the news. What's more, once someone finds out something, she can spread the word globally. But newsmakers need to embrace this new reality, not fight it.

They should also realize that they are far from helpless in the new era. They can use the same tools, in fact, to bring their message to the outside world, and to improve the way they communicate internally, as we'll see in the next chapter.

These changes are, at the least, disconcerting on all sides. However, I strongly believe that they are a positive trend because they encourage openness instead of paranoid secrecy. And in the end, like it or not, they're inevitable.