The written word has long been a revolutionary agent. Manifestos, treatises, even novels, have started riots, changed the course of history, and toppled governments. Writing is so powerful that when the rebels take to the streets, they head first to the newspapers, only later to the presidential palace.

In the sixteenth century, reformers nailed their handwritten complaints about the establishment to the church door. With the spread of the printing press, pamphleteers distributed their manifestos to the masses. In 1919, the anarchist Jacob Abrams set up a clandestine basement printing press in upper Manhattan to run off flyers in English and Yiddish protesting incursions of American troops into Russia at the end of World War I. The printed flyers were sprinkled from the rooftop of a building to be picked up by passers-by below. For their act, Abrams and four others were convicted of sedition under a recently-passed amendment to the Espionage Act. Their conviction was upheld by the US Supreme Court in a landmark First Amendment case, Abrams v. United States, with important dissents from Oliver Wendell Holmes and Louis Brandeis.
The dissidents of my youth cranked out their discontent on cheap, untraceable basement mimeograph machines. Today they use Twitter to destabilize the world, 140 characters at a time.

Or at least that’s what the mythology of technological innovation would have us believe, as it generates terms like #twitterrevolution to describe the Arab Spring, the Green Revolution, the Occupy Movement, the Umbrella Protests, and other contemporary uprisings. Terms like #twitterrevolution are so powerful because we imbue the internet with the transformative power to banish ignorance, foster democracy, and bring about world peace.

We had the same high hopes for manuscripts when they first appeared several thousand years ago,
and for the printing press, when it transformed communication, but as we wait for world peace, which still seems a long way off, we must recognize that communication technology is always a vehicle both for free speech and for censorship; for liberation, but also for oppression. The printing press enabled the *Communist Manifesto*, but it also gave us the Index of Prohibited Books.
Television revolutionized more than entertainment. It brought images of the Vietnam War to American living rooms, catapulting the antiwar movement from radical fringe to mainstream opposition. But as George Orwell foresaw, TV proved a terrific device for surveillance. Everyone within its view becomes a potential criminal, though the spying is sometimes tempered with the message that this will keep you safe.

Here, by the way, is what happens when you get caught in the sights of Chicago’s infamous red-light cameras.

Instead of stopping you to ask, “Where’s the fire?” police can now send you your traffic citation in the mail, along with a link to an online video of you—or whoever’s driving your car—brazenly breaking the law.

The internet, the latest in our communication technologies, creates opportunities for unfettered, widespread, even revolutionary expression. But like its predecessors, it offers the opposite as well: opportunities for surveillance and censorship—both
government and private—on a scale never before imagined. The computer and smartphone are our windows on the world. But they’re also the new panopticon: what we do on our mobiles and laptops gives that world a fairly detailed look at who we are, where we are, and what we’re up to. Based on that information, people try to sell us things we may not need; they try to stop us from doing what they don’t like; in extreme cases, they even track us down and lock us up.

One popular feature of the ’net, social networking, has particular revolutionary potential: it lets dissidents connect with one another and coordinate their efforts to overthrow the régime, and it gives them a way to signal their discontent to the outside world. At least, that’s how it seemed to work during the Arab Spring of 2011. But communication works two ways, and whether or not they “friend” us, governments seem eager to track our status, check out our photos, check up on our friends. It’s not hard to do: with just a few clicks, the governments of Turkmenistan, Brunei and Bahrain conduct domestic surveillance of their online political dissidents using repurposed off-the-shelf software designed for catching crooks. But as we will see in a minute, liberal democratic governments spy on their citizens as well.

Livetweeting the revolution

With the whole world going digital, it’s easy to get carried away and call the success of the Arab Spring the #twitterrevolution, complete with hashtag. After all, Twitter, Facebook, and YouTube seemed inseparable from the unrest in North Africa and the Middle East which started in December, 2010, and eventually saw leaders ousted in Tunisia, Libya, Egypt, and Yemen, together with unrest in Bahrain, and in Syria, where the fall of the regime is expected any day now, or maybe not.

Manuel Castells has even argued that Iran’s green revolution “began on the Internet social networks, as these are spaces of autonomy largely beyond the control of governments and corporations” (2012: 2). Former U. S. National Security Advisor Mark Pfeiffle claimed that, “Without Twitter the people of Iran would not have felt empowered and confident to stand up for freedom and democracy” (quoted by Gladwell, 2010). Most
recently, Philip Howard argues that digital media was “consistently one of the most important sufficient and necessary conditions” for the Arab Spring movements (2013).

And on its 7th anniversary, Twitter included this Arab Spring image in a slideshow of Twitter milestones.

But all that seems much too optimistic. As Castells himself reminds us, historically, governments and corporations “monopolized the channels of communication as the foundation of their power.” Unfortunately, that’s still going on: business and government continue to clamp down on internet communications, social networking in particular. Less than two years after the Tahrir Square uprising, a prominent Egyptian pro-democracy blogger was arrested because someone mentioned his name in a tweet, arousing suspicions that he was engaged in activity against the Muslim Brotherhood.

But even without such clampdowns, many scholars are skeptical about Twitter’s revolutionary power. Malcolm Gladwell reports that most of the tweets about the Iran election came from outside the country and were in English, not Farsi. For Gladwell, social media require little in the way of commitment: it’s easier to “like” the revolution
online than to actually man the barricades, a phenomenon that has come to be called “slacktivism.” And even if social media do connect us, Ethan Zuckerman (2012) warns, that in itself won’t “automatically lead to increased understanding.” Zuckerman points to the words of Guglielmo Marconi, inventor of the first kind of wireless, whose 1912 prediction that radio “will make war impossible, because it will make war ridiculous” was proved wrong only two years later by the outbreak of World War I.

But that doesn’t stop futurologists from embracing social media as a force for revolution and liberation. Dreamers like Castells might wonder, What if Rosa Luxemburg had 20,000 Facebook friends? What if Che Guevara had a Blackberry in Bolivia? What if the Tank Man of Tiananmen Square had a Tumblr?

How many clicks does it take to topple a régime?

Technologies from the printing press to the internet, while they’re never strictly neutral, can be counter-revolutionary as well as revolutionary. Even writing itself—the essential
literacy technology—functions as an agent of bureaucracy and empire, arranging society into hierarchies of castes and classes. Claude Lévi-Strauss (1961, 290-92) goes so far as to call writing more a tool of enslavement than enlightenment. That’s an extreme position, but it’s clear that although writing can inspire reform and lead to democracy, it can also advance autocratic government agendas, suppress controversy, quash revolution, and punish unbelievers.

Looking back at the events of the recent revolutions, it’s clear that although Twitter and Facebook may have played a role, digital technology didn’t cause the upheaval. And it’s also clear that governments used the same digital tools to push back against insurgents, tracking locations, capturing images, taking names.

That doesn’t mean technology’s not a game changer. Egypt saw the ouster of long-time strongman Hosni Mubarak, and a local Google employee, imprisoned for rallying the opposition on Facebook, even became for a time a hero of the Tahrir Square insurgency. The Twitter Revolution was similarly credited with ousting Tunisia’s long-time President Ben Ali. Social media supported Iran’s green protests, and they have been instrumental in other outbreaks of resistance in a variety of totalitarian states elsewhere as well.

But statistics suggest that clicks alone won’t topple a régime. Only 11.4% of Egyptians actually use Facebook, and the crowds in Cairo’s Tahrir Square continued to grow during the five days that the Mubarak government shut down the internet. In Tunisia, too, it took more than a wireless connection to effect political change. Tunisians ousted their leader though only nineteen percent of them had online access, compared with more than 46% in Iran, where the #twitterrevolution fizzled. Because even in Iran, whose futile protests may have been tweeted ’round the world, there were few tweeters actually in-country, not enough to counter government forces and the religious oligarchs who run things.

And of the 450 million Twitter users worldwide, only 0.027% of them live in Egypt, Yemen, and Tunisia (Curran et al, 2012). The Middle East, the current hotbed of protest, has an internet penetration of 35.6%, low compared to 61.3% in Europe and 78.6% in North America, where revolution seems unlikely. And finally, whether or not the revolution in the Middle East was digital, it’s far from clear that the Arab Spring will lead to actual democratic reform.

Plus while many of us can’t seem to survive without the constant stimulus of digital multitasking, much of the world barely notices when the cable is down, being preoccupied instead with raising literacy rates—the internet is useless if you can’t read—as well as fighting famine and disease, and finding clean water, not to mention a source of electricity that works for more than an hour every day or two.

In contrast, the “radical” internet belongs to the well-educated, economically comfortable middle classes with the resources, and the leisure, to click a link or kvetch when things don’t go their way. And speaking of first-world problems, it takes more than a “like” or a retweet to get the bourgeoisie running in the streets.

#twittercounterrevolution
Perhaps we should speak instead of the #twittercounterrevolution? Because, for every revolutionary manifesto there’s a volley of government propaganda. For every eye-opening book there’s an official do-not-read list—or worse yet, a bonfire. For every
phone tree organizing a protest rally, there’s a warrantless wiretap waiting to throw the ralliers in jail.

And for every revolutionary internet site there’s a filter, like the Great Firewall of China, blocking sites and tracking users considered dangerous by the authorities. In the case of Egypt, there was a simple switch that shut down the web. North Korea permits extremely limited access to the internet, offering residents instead a tightly-controlled intranet called “Red Star” that links only to approved sites and a new, Facebook-like message board. Prompted by a recent visit from Google’s Chairman, Eric Schmidt, North Korea agreed to permit foreigners—though not North Koreans—to send data over Koryolink, North Korea’s new 3G mobile service (Dewey 2013).

In Cuba, only 23% of the island’s 11.2 million residents have permission to use the government-controlled intranet, not from home but at licensed computer clubs, and the Castro régime still prohibits mobile internet, though only 22% of Cubans have any sort of telephone at all. Tourists are apparently exempt from mobile phone controls in Cuba, but according to TripAdvisor they’ll have trouble finding a mobile data connection and will pay heavily for every painfully slow megabyte they use.

Perhaps the most dangerous counterrevolutionary tactic is to take the very tool that allows revolutionaries to interact and use it to hunt them down. Mainland Chinese authorities have routinely tracked the online activities of dissidents, throwing high-profile bloggers in jail to discourage others. Now, Hong Kong has begun to do the same. Police have arrested pro-democracy “Umbrella movement” protestors who post calls to action online for violating a law prohibiting the use of a computer “with criminal or dishonest intent.”
**Tweet level orange**

But it’s not only dictatorships that block, restrict, or monitor social media traffic. In 2010, a British accountant named Paul Chambers tweeted his frustration over a snowbound airport:

> Crap! Robin Hood airport is closed. You’ve got a week and a bit to get your shit together, otherwise I’m blowing the airport sky-high!

The airport security chief came across the tweet several days later, while surfing the ’net at home, and alerted the police. Chambers was arrested, convicted of sending a menacing message in violation of the 2003 Communications Act, and fined £1000 by a humourless judge. After the incident went viral and attracted the support of television celebrity Stephen Fry, the appeals court reversed Chambers’ conviction.
Closer to home, a division of the U. S. Department of Homeland Security regularly scans Twitter and other internet sites, looking for words from a watch list of about 500 terms popular with terrorists (see pages 20-23 of this link). Tweeting one of these words could jump your threat level up from green to red in 140 characters or less. But you can be busted for tweeting anything even remotely suspicious. That’s what happened to two British tourists, Leigh Bryan and Emily Bunting, who were denied entry to the United States for inappropriate tweeting. The would-be tourists were interrogated by Customs and Border Protection agents for five hours at Los Angeles International Airport, handcuffed, locked up overnight with scary tattooed drug dealers, and sent back to England in the morning. All this because, before their visit, Bryan tweeted to a friend using words that attracted the attention of Federal terror watchers.

The offending tweets read, “3 weeks today, we’re totally in LA p*****e people off on Hollywood Blvd and diggin’ Marilyn Monroe up!” and “free this week for a quick gossip/prep before I go and destroy America?”
According to Bryan’s “denial of entry” form,

Mr. BRYAN confirmed … that he was coming to the United States to dig up the grave of Marilyn Monroe. Also on his tweeter account Mr. BRYAN posted that he was coming to destroy America.

Bryan explained to his interrogators that he meant none of that literally, that destroy is British slang for partying and getting drunk, and “digging up Marilyn Monroe” is a reference to the American TV show, *Family Guy*. The humorless border agents actually searched the suspects’ luggage looking for the shovels the suspects planned to use to exhume Monroe.

Bryan and Bunting were detained, interrogated, and stamped “return to sender” because the American government diligently scans social media in an effort to stop terrorist activity before it starts. *Destroy* isn’t on the watch list of the MMC—the Media Monitoring Capability group tasked with alerting their superiors to IOI’s (Items of Interest) that they find when reading social media. The list has nothing about Marilyn Monroe, either. But some Twitter-reading algorithm, or possibly a snitch, tipped off the feds to Bryan’s vacation plans, and before they could do any serious damage, agents were able to intercept the couple at LAX—the feds suspected that his companion would act as the lookout for the Marilyn Monroe exhumation. Needless to say, Bryan didn’t get to do any serious partying either.

The DHS watch list contains words clearly associated with terrorism, like white powder, Ricin, Al Qaeda, Hamas, and jihad. However, much of the list consists of words likely to be harmless: interstate, ice, dock, smart, subway, electric, vaccine, wave, and cloud. Cuba, China, and Iran are on the list, but so is San Diego. There are cyber words on the watch list: hacker and worm, for example. But Facebook founder Mark Zuckerberg might be surprised to learn that the phrase social media itself is on the social media watch list. Using it in a post could definitely trigger an Item of Interest from your watcher.
It goes without saying that the Department of Homeland Security must do its best to keep America safe, and DHS invades no one’s privacy when it scans the web, because anyone posting to a public site has no reasonable expectation of privacy. No one doubts that online posters who make demonstrable threats, stalk, or otherwise harass victims online, or conspire on the internet to commit crimes, should be stopped and punished. But now ordinary web users, who aren’t terrorists or cybercriminals, must not only worry how many words they can fit into Twitter’s 140-character straightjacket, they must also consider whether their words will bring a knock on the door in the middle of the night.

Here’s an innocuous enough tweet:

Agent: film screening a disaster. New organization, closure would aid plot. Send edits to cloud, target social media to help explain delays.

It contains 140 characters forming 22 words, 59% of them on the DHS terror-word watch list. I’ve marked them in red to indicate their threat level. Nevertheless, even if someone tweeted this, there’s not much chance that a computer would flag them at the border. That’s because, unless we’re thinking this is some super-secret spy code, a human reader would probably find no contexts in which the watch-list-heavy tweet would raise an alarm.

The real problem with terror word lists comes not from jokes that fizzle, but from the fact that although English is still the most commonly-used language on the internet, it is not yet the official language of international terrorism.

Leigh Bryan wasn’t in an airport or anywhere near L.A. when he tweeted his vacation plans in terms that alarmed American border guards. There was plenty of time for security analysts to figure out whether he posed a credible threat to the Hollywood hills. Plus the absence of shovels in the travelers’ luggage might have furnished a clue. But as Bryan found out, in the digital age, getting there is not half the fun. Might as well stay home and get on Facebook—he can’t get back on Twitter: that account is closed.

**Elonis v. United States**

In the US, a Facebook post can land you in jail. In 2010, Anthony Elonis was convicted of posting Facebook threats against a number of people: his estranged wife, Tara, after she took out an order of protection against him; an FBI agent who had attempted to question him about his menacing Facebook posts; unnamed police officers who had yet to do anything to annoy Tony Elonis; and an unspecified kindergarten class, one within a ten-mile radius of Elonis' home. He was found not guilty on a fifth count of threatening co-workers at the amusement park where he no longer worked—the jury didn’t think those Facebook posts constituted true threats. It wasn’t a watch list, but the amusement park’s manager, who saw the posts on Facebook, who first alerted authorities.

The law Elonis violated, the Interstate Communications Act, makes it illegal to threaten someone across state lines. The government contends that Elonis’ words inspired fear in those who read them, but Elonis insists he didn’t mean to threaten anyone. He wants to be judged by his intent, not by how readers perceived his posts. For example, when he posted,
If I only knew then what I know now . . . I would have smothered your ass with a pillow. Dumped your body in the back seat. Dropped you off in Toad Creek and made it look like a rape and murder,

he didn’t intend to threaten his estranged wife, that was just therapeutic venting after a bad breakup. And when he wrote,

That’s it, I’ve had about enough
I’m checking out and making a name for myself
Enough elementary schools in a ten mile radius to initiate the most heinous school shooting ever imagined
And hell hath no fury like a crazy man in a Kindergarten class
The only question is . . . which one?

he didn’t intend to shoot up a school, even though his post put local schools on alert. According to Elonis, he was just channeling the violent lyrics of the rapper Eminem. Some of Elonis’ rants linked to the Wikipedia entry on freedom of speech, and so, he argued, his posts should be protected by the First Amendment. But a jury didn’t buy it, sentencing Elonis to forty-four months in jail, and the circuit court upheld his conviction on appeal. He served three years, followed by another three years of restricted activity while under court supervision.

Elonis is currently appealing his conviction to the US Supreme Court, which heard oral arguments on Dec. 1 and will decide the case later this term.
DARPA, the Defense Advanced Research Projects Agency, is pursuing projects that make watchlists and snitches obsolete. The goal of TIA, the “Total Information Awareness Program,” is,

to imagine, develop, apply, integrate, demonstrate, and transition information technologies . . . that will counter asymmetric threats by achieving total information awareness useful for preemption, national security warning, and national security decision making.

(Now that’s a sentence that should set off alarm bells, not at border crossings, but in the English teachers lounge.)

TIA is a data-mining tool for preventing terrorist attacks like the ones of 9/11. But the Wall Street Journal speculated that deploying a program like Total Information Awareness, which crunches online interactions looking for suspicious patterns—for example, gun purchases accompanied by “how to make a bomb” searches—might also have been able to stop the mass shooting in an Aurora, Colorado, movie theater, considering that the killer left an online trail that, if interpreted correctly, could have set off alarm bells.

And the Guardian reports that a few American police departments are trying out the kind of algorithm that Amazon dot com uses to sell books in order to better predict not just where and when a crime might take place, but also who is likely to commit it. Of course crooks could benefit from the software too. Entering the search term petty theft could prompt the message: Crooks who like breaking-and-entering might also like great bodily harm.

DEFT, which stands for Deep Exploration and Filtering of Text, is a U.S. Defense Department program to understand “connections in text that might not be readily apparent to humans…. Sophisticated artificial intelligence of this nature has the potential to enable defense analysts to efficiently investigate orders of magnitude more documents so they can discover implicitly expressed, actionable information contained within them.”
The DoD also sponsors BOLT, for Broad Operational Language Translation, a program whose goal is to create “new techniques for automated translation and linguistic analysis that can be applied to the informal genres of text and speech common in online and in-person communication.”

Six degrees of separation: RIOT knows your friends, and their friends, and their friends.

The most recent addition to this battery of social-data crunchers comes from DoD subcontractor Raytheon, which has developed RIOT, or Rapid Information Overlay Technology. According to the Guardian, “the same social networks that helped propel the Arab Spring revolutions can be transformed into a ‘Google for spies’ and tapped as a means of monitoring and control.” RIOT works by scanning and analyzing social media to locate where users have been, where they are now, and where they might be going. It can track bad actors, and it can track you.
Locations of a Raytheon employee based on social media site check-ins.

**Selling the #twitterrevolution**
The Egyptian revolution was up on Wikipedia faster than you could say Wolf Blitzer. But government surveillance and control of communication channels are only part of the problem facing internet users. There’s tight commercial control of our communication technologies as well. Consider the typewriter:
Like today’s internet, the typewriter, was billed as revolutionary when it first came on the scene, as we see in this 1875 ad for the Remington “type-writer” that ran in the *Nation*. The text being typed is from Shakespeare’s *Julius Caesar*: “There is a tide in the affairs of men which, taken at the flood leads on to fortune.”

![Image](https://example.com/image.jpg)

That’s a line spoken by Brutus, the dissident who assassinated the tyrannical Caesar during that earlier, Roman, spring, a couple of thousand years ago, and it’s used in the ad to underscore the revolutionary power of the newly-invented writing machine.

But there’s a difference: the fortune being touted by Remington is not political, it’s financial. Typewriters aren’t rabble rousers, they’re job creators. The advertising copy describes the typewriter’s transformative power:

> No invention has opened to women so broad and easy an avenue to profitable and suitable employment as the Type-Writer.

And Remington’s pitch closes with a call, not to enlist in the revolution of the working classes, but for a few highly-motivated regional sales reps—despite the gender revolution heralded by the typewriter, these are presumably *salesmen*, not *women*—to sign up and sell the new machines, a job, we’re told, that’s certain to be “safe, sure, and profitable.”

Similarly, whatever role today’s revolutionary internet technology may have in supporting political revolutions, it’s clear that one of its primary functions is to target both revolutionaries and their oppressors with context-sensitive ads. In fact, the tight *commercial* control of the internet, together with the ever-increasing corporate emphasis on protecting intellectual property in cyberspace, is potentially more significant than government surveillance, particularly for today’s armchair revolutionaries.
Companies like Google and Microsoft argue strongly for a free and open internet—one of Google’s basic business principles is, “the need for information crosses all borders.” But paradoxically, this freedom of information is managed with top-secret formulas, at locked-down corporate HQs and server facilities that are strong enough to survive a nuclear attack, not to mention the revolution of the proletariat. Add to this the phenomenon of digital-rights-managed music, video, and now ebooks, and we find that the electronic frontier is being fenced in, and the information superhighway is fast becoming a limited-access toll road.

Although many of us are quick to complain about government surveillance of our internet or mobile phone use, because that’s an invasion of our privacy, we don’t seem to mind corporate intrusions as much. When Google records our keystrokes and sells that data to advertisers, or YouTube warns us that we may be violating copyright, or Amazon suggests a similar novel we might also like to read, we’re less likely to grumble, because, hey, that’s just capitalism working the way it’s supposed to work.

So, for the complete digital revolutionary experience, abandon the underground presses, don’t bother with the radio stations. The next time you have the urge to take your protest to the streets, just send out an Evite. You can check Facebook and Twitter to see who’s coming.

**Conclusion: Welcome to the digital revolution: click here to accept our terms of service.**

Today’s activists know that before you lead the revolution online you must first agree to your internet service provider’s terms of service. These tend to be long documents written in dense legal language designed *not* to be read. In fact most people never read them:
because life is short. I mean, where would Cuba be today if Fidel Castro had to click “agree” back in 1959 before overthrowing the Batista régime?

But before you commit to the online revolution, it might just be worth looking at the fine print. Since revolutions are known to be harmful to your health, the 20,000 word end-user agreement for AT&T’s ISP contains this legal disclaimer:

7. INDEMNITY

You agree to indemnify and hold AT&T and its subsidiaries, affiliates, directors, officers, agents, and employees harmless from any claim, demand, action, citation, or legal proceeding, including, but not limited to, those arising out of or resulting from the death or bodily injury of any person, or the damage, loss, or destruction of any real or tangible personal property, or for reasonable attorneys’ fees (except as provided in paragraph 11(e) below), made by any party against AT&T, its subsidiaries, affiliates, directors, officers, agents, and employees arising out of or related to your use of or inability to use the Services, your connection to the Services, the provisioning or alleged failure to provision the Services, a violation of any provision of this TOS, or your violation of any rights of another.

In plain English, that means the company’s not responsible if you die because you used the internet, or because you couldn’t get online.

Similarly, #twitterrevolutionaries must first accept Twitter’s own limitation of liability:

[Twitter] … disclaim[s] all responsibility and liability for: … losses, resulting from (i) your access to or use of or inability to access or use the services; (ii) any conduct or content of any third party…including without
limitation, any defamatory, offensive, or illegal conduct of other users or third parties.

In plain English, Twitter is not responsible for the technical glitches that plague the internet, or if your tweet produces an adverse reaction in one of your tweeps. Our corporate sponsors want to welcome you to the digital revolution, but don’t come running to us if the revolution fails because the network is down.

Even if the government watchdogs don’t manage to intercept our network traffic, and Twitter doesn’t turn our account information over to the authorities in response to a subpoena, as they did recently with the Occupy Wall Street tweets, all Terms of Service (TOS) agreements hold providers harmless for the many interruptions in service that plague our online lives. So no matter if our ranks are swelling, we may still have to put the revolution on pause simply because the server crashes when we need it most.
Oh, and if it’s the #twitterrevolution of the masses that you’re aiming for, just remember, Twitter has no phone number for customer service, so when Twitter goes down, good luck calling tech support.
Works cited


