‘Secrecy is for losers’: why diplomats should embrace openness to protect national security

Alexis Wichowski
Columbia University / US Department of State

Introduction

> “Secrecy is for losers. For people who don't realize how important information really is…We put [openness] in peril by poking along in a mode of an age now past. It is time to dismantle government secrecy. It is time to begin building the supports for the era of openness that is already upon us.”
>
> – Senator Daniel Moynihan (*Secrecy*, 1998)

The digital landscape is a leaky place. And in it, government just can’t get away with what it used to. While bad behavior by governments has always been outed eventually, in the digital era it’s easier than ever to reveal even peace-making government activities, whole hog and in real time. Exposure in the digital landscape, for good or for ill, is simply much, much easier these days.

This scares the pants off government. Which is understandable – the digital landscape is complicated, and complicated things bring complicated new threats. Some parts of government seem to think the safest thing to do is in the face of this complicated new landscape it to just kind of avoid it. Leave the share-everything social-networking to regular folks, and inside government – and in the diplomatic and national security agencies especially – just share less. In a quest to be safe, government is becoming more secret. And secrecy is not just a practice, but a culture; an operational mode of being.

This chapter argues that this is a mistake. A culture of secrecy undermines diplomacy by shuttering up windows diplomats need kept open. And in the digital era where information-sharing is an increasingly normal part of daily life, it’s not going to work anyway.

This chapter will describe in detail why not. But first, some context from recent events:

In June 2013, federal contractor Edward Snowden leaked roughly 200,000

> classified documents describing activities of the US government’s National Security Agency, better known as the NSA. Chief among them were papers detailing a digital surveillance program known as PRISM: a massive data collection sweep that scooped up phone records of millions of US citizens – whether they were suspected of crimes or not.
>
> US national security agencies responded to all this with some serious soul-searching. First, they looked at the surveillance practices themselves. The surveillance, they found, may have in fact been illegal.[1] And even if it wasn’t, it wasn’t all that effective, terrorism prevention-wise[2]. Government investigators also looked at their own workforce – the millions of federal employees like Snowden who have access to classified information[3]. The results of investigation after investigation keep circling the same conclusion: the digital landscape is a new world, with new threats. And old ways of dealing with the threats aren’t going to work. As former Assistant Secretary of Defense Paul Stockton wrote, the idea that “if we build a fence around us, we’ll be secure…is outmoded. It’s broken and it needs to be replaced” (Cooper, 2014).

Diplomacy doesn’t deal with physical fences, but the metaphor holds up: the idea that erecting a culture of secrecy around diplomacy will keep a nation secure is outmoded. It’s broken. This idea needs to be replaced.

Note, this chapter does not argue that “secrets” are bad, but rather that “secrecy,” as a culture within which to operate, is. This chapter will explore why this is at length, but summed up, it is because the world at large no longer lives in a dominant mode of secrecy. The global population is increasingly tied to a digital landscape where information-sharing, not secrecy, is the norm, both as practice, and as principle. Diplomats need to adapt to the digital landscape, and a culture that discourages them from sharing information both within and outside government undermines their ability to do so.

Fifteen years ago, Senator Daniel Moynihan wrote, “Secrecy is for losers… For people

[1] In December 2013, a federal judge presiding over *Klayman v. Obama* ruled that the PRISM data collection practices may have violated citizen’s constitutional rights. (NBC News, December 20, 2013). On January 3, 2014 the government filed an appeal (USCA Case #14-5004). .

[2] The White House report on PRISM, prepared by a task force handpicked to assess the pros and cons of the surveillance program, concluded “There has been no instance in which NSA could say with confidence that the outcome [of a terror investigation] would have been any different” without the surveillance (“Liberty and security in a changing world: report and recommendations of the President’s Review Group on Intelligence and Communications Technologies,” 2013).

[3] This was a long time coming; Snowden wasn’t exactly unique in using his security clearance for non-approved purposes. Three years prior to the NSA leaks, Chelsea (then Bradley) Manning, a private in the US Army, used her active security clearance to download hundreds of thousands of classified diplomatic cables. And three months after the NSA leaks, in a far grislier manifestation of abusing a security clearance, Aaron Alexis, an honorably discharged Naval reservist, used his still valid security clearance to gain access to a Navy yard in downtown Washington DC where after being approved to walk through the front gates proceeded to shoot and kill 12 people.

who don't realize how important information really is…We put [openness] in peril by poking along in a mode of an age now past." To secure a nation, governments cannot retreat into the outdated mode of secrecy. They must come to grips with the mode of openness that defines the age it's in.

The context

Let's start with a good hard look at the age. On an average day in 2013, 144 billion emails and 19.1 billion text messages were sent (Clark-Dickson, 2013). On an average month, 1.19 billion people went on Facebook, 1 billion watched videos on YouTube, and 232 million used Twitter via 2.7 billion internet connections and 6.7 billion mobile phones (Granger, 2013; Radicati & Buckley, 2012; YouTube: Statistics, 2014). Internet use is up 566.4% in the past decade and a half (Internet world stats, 2014).

These statistics show two things: first, the digital environment creates immense opportunities for people to share; and second, many people are doing just that. They voluntarily share links to things they've read or watched, their opinions about the things they've read or watched, or even original new works for others to read and watch. But they also share information about themselves: run of the mill stuff like professional titles, associations, and specializations; but also personal information, from digital versions of kids and spouse pics to self-inflicted Orwellian "check-ins" pinpointing one's own exact location at an exact moment. The digital landscape -- both the tools in it and the culture that has risen up around it -- make information-sharing of all kinds simply *more*: more possible, more likely, more normal.

It may seem like knowing about general information-cultural norms are all well and good, but the more important issue for diplomacy is isn't the sharing of run of the mill information but the sharing of sensitive information: practices and confidences whose public exposure could undermine relationships with allies, embolden enemies, and weaken the state. Not so. This chapter argues that information-sharing culture and the preservation of sensitive information are inextricably linked. To understand this link, let us examine who's doing what in the digital landscape, what they're doing, and why.

The who

Tools are important. They enable action. But it's necessary to also examine the people who *use* the tools: the agents of action. This involves taking stock of the roles they inhabit and the motivations that drive them. The "who" in this chapter consists of three broad categories: government, leakers, and the community of civilians to whom leaks are revealed.

First, to clarify terms. The concept "government" is too broad for in-depth examination. When the term "government" is invoked in this chapter, it means the foreign policy wings of government: diplomatic institutions and defense agencies, the two areas of government most responsible for protecting sensitive information and preventing leaks.

"Leakers" is a more specific category. They are, simply, people who reveal secrets that they're not supposed to; in this case, government secrets. When public opinion is on their side, they tend to be called "whistleblowers"; when not, "traitors." This chapter will use the term "leakers" as an intended neutral label, describing this group of individuals by their actions alone.

Leakers, however, are not a distinct, stand-alone group. They're invariably entangled in some way with the first and third groups. They are part of the community of citizens. They're also necessarily part of the government: soldiers, like Chelsea (formerly Bradley) Manning, who initiated "Wikileaks[4]"; contractors, like Edward Snowden, who orchestrated the NSA leaks; or analysts, or operatives or a myriad of other role types which will be explored further on. While to the public, leakers may be regarded as just that – He Who Leaked Classified Information -- to understand why a culture of secrecy is a bad idea for national security, leakers' roles as citizens and as agents of government must be borne in mind as well.

The third group, as mentioned, is the community of citizens; the broad net of people to whom leakers heave their catch. Here I refer not just to "the public" but rather two fairly distinct subgroups of it: 1. citizens who promote information-sharing as a right; and 2. working-level government officials. This chapter explores these roles in depth.

"Digital" diplomacy

This sums up the "who": government, leakers, and citizens. And the "what" is the secrecy-openness balance whose calibration these groups seek to adjust. The "where" and "how" are tougher to pinpoint, but I suggest that term "digital diplomacy" is a way to get at them. "Digital diplomacy" describes diplomatic activities (the diplomacy) that move along bit-enabled axes (the digital).

At the same time, the "where" and "how" in "digital diplomacy" are a bit of a Schrödinger's cat: these activities are both of and not of a place, referring to diplomatic activities both in countries, and not in countries. And it both is and is not of a particular technology: "digital" suggests the *presence* of a connection technology, but this could mean a possible as well as an actual presence. For instance, the awareness that some narrative *could* go "viral" affects a diplomat's decision-making calculus in many contexts, whether a digital tool is actually being used or not.

Thus, digital diplomacy is perhaps best described not as a medium, but a mindset. Marcus Holmes and Corneliu Bjola aptly describe it as "a way for states to manage change" (2014). Sometimes this change is better managed with technology, but not always. Push-pull media can sow a narrative or collect data, but it hasn't replaced the coffee meeting.

[4] "Wikileaks" refers here to the November 2010 event in which 251,287 classified diplomatic cables were made public, not the activist organization who assisted Manning in doing so

Like any tool, digital is good for some things and not so good for others. Knowing what tool would work when; that is the art of diplomacy. Knowing how the digital environment influences this art; that’s digital diplomacy.

Information-sharing as a cultural value

Information-sharing comes of age

Having established the whos and hows of the digital information-sharing age, it is now time to take a look at how they got here. People have shared information with each other in some sort of recorded, shareable form -- as opposed to spoken, ephemeral form -- for thousands of years[5]. Other options didn’t really present themselves until long-distance phone service went mainstream after the 1950s. But even after the phone, written correspondence in the form of letters remained most people’s primary means for keeping in touch with far-off friends, relatives and colleagues for the next few decades (Schmid,, 2011).

As the home phone became integrated into American life, people communicated to each other via writing less and less. They could just call -- it was easier, and got cheaper with each passing year. According the US Postal Service’s first annual Household Diary Study designed to study mail patterns, by 2011 the average American household sent or received only one (1) unit of personal correspondence[6] every two weeks (Mazzone & Rehman, 2011).

The letter-writing drop-off did not mean, however, that Americans en masse just anti-socially bowled alone. While communication in the form of mailed letters dwindled, communication in other recorded, shareable form soared. Let’s preserve the two-week time frame used in the US Postal Service study for comparison purposes. In an average two-week period in 2011, while Americans only sent or received 0.7 units of correspondence in physical form, they exchanged 4,942 units of correspondence in digital forms[7]: specifically, an average of 812 emails (58 / day), 140 texts (10 / day) and 3,990 units of social media content (285 / day) (Bennett, 2013) (Smith, 2011).

It is worth pausing for a moment to consider what all this says about the culture of

[5] Admittedly, pre-digital era folks wouldn’t likely have characterized their written communication as “shareable,” but for context-setting purposes of this chapter it must be pointed out that technically, it was.
[6] “Personal correspondence” is defined in the study as “household to household mail” (p.21) that includes “personal letters, holiday greeting cards, non-holiday greeting cards, invitations/announcements, other personal” (2011, Mazzone, J. p.24)
[7] The comparison is not precise: it is not possible to determine that the emails, texts, and social media content conform to exactly the same definition of “personal correspondence” that was used in the USPS study. However, I argue that these digital correspondence statistics are indeed fit for comparison purposes, for two reasons: 1. the email statistics represent individualized human correspondence, excluding spam and marketing newsletters; 2. in 2010 it was still illegal to text someone’s phone without their permission, making texts also a form of personal correspondence. Social media correspondence statistics are less clear, but many social media networks, such as Facebook, suggest a personal relationship between the users. Granted, others, like Twitter and YouTube, do not.

communication; not just in the US, but among humans. For the vast majority of history, interpersonal communication was oral, transactional (Fang, 1997). And for a really long time, writing remained the sole purview of a teeny slice of educated elites. Letter-writing among the non-super elite began to take hold around the 1840s with the introduction of the postage stamp, making letter-delivery possible for even the personal messenger-deprived masses (Garfield, 2013).[8]

We know all this for two reasons: first, because the information was recorded; and second, because it was saved. Now, for all but the last handful of decades, recording was a huge pain. It required either being literate or getting someone else who was to put chisel to stone or quill to parchment. So, as archeological evidence and good horse sense tell us, ancestral scriveners didn't just record any old thing. To be recorded, information had to be important: from laws of the lands to ledger books. In short, not everyone could make information a physical form, and not every bit of information was deemed form-worthy.

So -- and this is the big so-what to this aside -- for most of human history, what regular people communicated was simply not recorded; and un-recorded, it couldn't be readily shared. But let's assume for a moment that regular folks' communications might have been recorded and could have been shared: who would read it? Who would want to? The notion that writings of the non-elites might be of interest to masses of anonymous others -- not out of sentimental value for sender-receiver but because the information itself had some value as a public good -- is difficult to imagine.

It's different now. Thanks to the digital revolution, recorded information's reach has expanded from the elites to the everyman in just a few decades. And sharing that communication virtually effortlessly went from inconceivable to being an every other minute[9] activity since the dawn of social media in the last decade. Given this context, I submit it is reasonable to assert that information-sharing is now, in 2014, a firmly planted new normal for the vast majority of the developed world[10].

"Information wants to be free"

For some in the developed world, however, information-sharing is not just the new normal. For some, information-sharing is a right. It's something to believe in; a cause to fight for.

[8] Apparently some elites bemoaned the postage stamp for contributing to the "cheapening of an art form." As Simon Garfield notes in "To the letter: a celebration of the lost art of letter writing," in the 1919 Yale Review lament on the dying art of letter-writing, blame was also laid on the telephone, the typewriter, the telegraph and even the train (for delivering letters too quickly).

[9] Literally: derived by assuming 16 waking hours in an average day, divided by 353 per day, totaling 22 per hour.

[10] With only about 35% of the world's population online, it must be acknowledged that those in developing nations may not yet experience information-sharing in the same way as those in developed ones. However, there are signs the gap will shrink quickly: in 2014, around 70% of people in developing nations have basic cell phones, and some marketers estimate that within five years about 60% of the developing world will have access to smart phones (*Internet world stats, 2014;* Fitchard, 2013).

It started in the '80s, and, not surprisingly, with one of the guys from Apple. Company co-founder Steve Wozniak was at a conference with a commune advocate named Stewart Brand. Brand had launched a magazine in 1968 called *The Whole Earth Catalogue* marketing a whole range of do-it-yourself, back-to-the-land type stuff, including specs on wood-fired stoves and instructions on how to build a yurt (1969). *Whole Earth*, however, was also one of the first places to advertise the Apple personal computer, regarding it as a tool like any other that could put power back into the hands of the people[11] (Leonard, 2014; Morozov, 2014).

At the first ever "Hackers Conference" in 1984, Wozniak and Brand casually discussed what would become a paradigm-shifting concept: "Information," Brand said, "wants to be free" (Edge@DLD, 2011). At the time, Brand was talking about how it would be increasingly difficult to charge money for information once digitized and so easily copied[12]. But as global networked computing became a reality, tech activists adopted the idea and took it as a mantra -- a literal one.

The reasoning behind the mantra goes something like this:

- Information, once digitized, is easy to share
- Digitized information is also easy to manipulate and search, from basic quotidian Google queries to sophisticated data mining
- This digital information searching reveals all kinds of valuable things, shockingly fast[13] – from patterns, research material, and regular old knowhow on how to do things
- Since digitized information can be shared with many people simultaneously and since it can reveal so many useful things, many people should be able to benefit from it as a kind of public good
- As such, information, the idea goes, should be free, and freely shared. In other words, information *wants* to be free.

Now, not everyone agrees with this; not least governments, who serve their citizens well by keeping some information secret, like who has what social security number or the identities of political asylum seekers. But bureaucrats were not in fact the first opponents of "information wants to be free." Opposition first came from the private sector.

[11] Evgeny Morozov wrote a critical but intriguing *New Yorker* piece on Brand, *Whole Earth* and the "Maker Movement," the 2013 outgrowth of World Earth's DIY activism. *Salon*'s Andrew Leonard laments Morozov's takedown in an enlightening rebuttal. Both are worth the read.

[12] Brand's full quote reads: "On the one hand, information wants to be expensive because it's so valuable. The right information in the right place just changes your life. On the other hand, information wants to be free, because the cost of getting it out is lower and lower all the time. So you have these two things fighting against each other."

[13] Fun fact: Google alone was queried 5,922,000,000 per day in 2013 (*Google annual search statistics*, 2014.). 15% of its daily queries -- 500,000 million of them -- had never before been asked (Farber, 2013).

This is perhaps best illustrated with the story of the Pirate Party.

Information-sharing as a movement

The Pirate Party grew out of an online peer-to-peer file-sharing site called The Pirate Bay, or TPB. Launched in 2003, anyone could use TPB to upload any content -- mostly videos, games, or music -- and anyone else could then download any of it for free.

As TPB became popular in the late 2000s, copyright holders of the freely-downloadable videos, games and music began to catch wind of what was happening with their works. Much of the publishing and licensing establishments saw peer-to-peer file-sharing as theft, plain and simple. And they saw file-sharing sites like TPB as not only abetting theft, but doing so aggressively and on a massive scale.

In 2009, the Motion Picture Association of America (MPAA), the Recording Industry Association of America (RIAA) lobbied hard for a crackdown on the TPB. It worked. That year, the four founders of The Pirate Bay -- Rick Falkvinge, Peter Sunde, Gottfrid Svartholm, and Marcin de Kaminski -- were tried in their home country of Sweden and convicted of copyright infringement (Pfanner, 2009; Swartz, 2009).

The MIAA and RIAA may have seen TPB as just a landing pad for thieving, but to the TPB organizers, file-sharing was more than a practice; it was a belief. They believed “information wants to be free,” and believed others did too. So when the four founded TPB in 2003, they also established the Piratbyrån, translated as “The Bureau of Piracy.” This is perhaps best described as a “loose collective.” In the words of the founders, it’s “not an organization,” per se, but rather, “an ongoing conversation…reflecting over questions regarding copying, information infrastructure and digital culture” (Piratbyrån, 2007). TPB associates were among the first quasi-political digital groups to take up the “loose collective” mantle; others, like the hacker collective Anonymous, came later.

If TPB were just a website, jailing the four founders and shuttering the Piratbyrån should have spelled the end of the story. But both the site and the movement are very much alive. Fans have kept the site going over the last 5 years through a vast underground network, changing its domain name six times in 2013 alone to evade shutdown by the authorities. The Pirate Bay is still the most widely used file-sharing site in the world. At last count, it had 18,911,877 users (RT News, 2013; Pfanner, 2009).

While TPB’s collective, Piratbyrån, officially shut down in 2010, its affiliated political party, The Pirate Party, grew. Under the umbrella “Pirate Parties International,” PPI has active chapters in 62 countries at the time of this writing. Their electoral record is still thin, but gaining ground: PPI won 7.1% of votes -- 2 seats -- in the European Parliament in 2009, 8.9 % of votes in the Berlin state election in 2011, a senator seat in the Czech national parliament in 2012, and 5.1% of votes -- 3 out of 63 seats -- in the Icelandic parliament in 2013 (Beyer, 2014).

This story matters to national security because it helps to explain why retreating into a culture of secrecy isn't going to work. The fight to share information is not just a consumer preference; it's a worldview. And it's spreading.

Who leaks, and why it doesn't happen more often

To understand why diplomacy lists, siren-called, toward a culture of secrecy from an age long past, we have to talk about leaks. The digital landscape doesn't make leaks happen, but it enables them to happen on a cosmological scale. Like Big Bang-expelled particles in the physical universe, leaked information in the digital universe expands, accelerates, and is almost immediately non-retractable. Once the information is out, it's not possible to just burn some files and make the leak go away. Leaked information races to the far corners of digital space, irretrievable and order-altering.

This makes the digital landscape, as mentioned at the outset, scary for governments. And it's eminently understandable why that's so. In addition to the speed and scale of their spread, leaks of all kinds – big and small -- can get out and do damage; not just gargantuan ones like Wikileaks or the NSA leaks. Tiny sensitive tidbits, if leaked, are just as irretrievable as the big ones.

To prevent any leaks, then, national security institutions within governments logically take steps to self-fortify. As discussed earlier, this might include more physical defenses – fences –, more cyber defenses – firewalls. And it's not hard to imagine that it wouldn't seem like a bad idea to have some more psychological defenses, too; a healthy dose of pants-scaring for everyone who works with sensitive information with a subtle but palpable culture of secrecy.

It's not necessary, though. Because let's be honest: nobody loves government. That said, most officials in most countries aren't doing anything to undermine their own government. Fear of reprisals might account for the bulk of why not. Or it might just be too much work to bother trying. But as unfashionably un-cynical as this may sound, I submit that the reason most officials don't try to undermine their own government is because they believe that it would be wrong to do so. A heavy-handed hatch-battening culture that stifles information-sharing simply isn't necessary.

Perhaps the culture of secrecy isn't aimed at most officials, though; it may just be aimed to deter would-be leakers. Before we get to the leakers, though, let's take a closer look at government officials in general and the information-handling culture in which they work.

The government & its information

Information, in national security, is not just currency; it's current. Information is the force that powers decisions. Without information -- data, analysis, chatter, chatting -- diplomatic and defense agencies couldn't do much. Information enables identification of threats and allies, the confirmation of context and history; it makes possible the deliberation on and delivery of plans. Information is a governments' most valuable inorganic foreign policy asset.

The most valuable *organic* foreign policy asset is, of course, the people who use the information: government officials. Here, I temporarily muddy the taxonomic waters by collapsing "government" and "working-level government officials." For a moment, let's step back and consider a huge overgeneralization of government, lumping together defense secretaries and ambassadors with the legions of officials whose work orbits theirs. Doing so is necessary to make the following point: in democratic countries, such as the United States, the same information-handling rules apply to everyone in government. Everyone. Anyone with a security clearance – that is to say, absolutely everyone in government from the ambassadors to interns – is required by law to protect diplomatic information according to a very specific set of rules.

"Classified" describes one set of rules. For people who work in government, figuring out which information is classified is pretty easy – it's literally got the word "Classified" stamped all over it. But assuming for a moment it didn't, it'd be worth perusing the rulebook. In the US, the rules governing classified information appear in the form of Executive Order 12958.

According to Executive Order 12958, potentially classifiable information includes: military plans, weapons systems, or operations; foreign government information; intelligence activities; foreign relations or foreign activities of the US; scientific, technological and economic matters related to national security; nuclear materials- or facilities -related information; infrastructure vulnerabilities; weapons of mass destruction (Executive Order 12958 - Classified National Security Information, as Amended, 2003).

Some of this is straightforward: weapons stuff, secret; nuclear materials info, secret. But some of the categories are a bit vague. For instance, "foreign government information" and "foreign relations of the United States": this could include just about anything the State Department works on. Fortunately, "classified" and "unclassified" are not the only tiers of information-handling rules. The most important of the other tiers for this argument is information known as "Sensitive But Unclassified" (SBU).[14]

Introduced by President Jimmy Carter in 1977 and expanded considerably after 9/11, SBU-category information covers what it sounds like it would cover: information that's not a state secret, but shouldn't be broadcast willy-nilly. This includes a wide range of categories, the most obvious being personal citizen information, like social security numbers, medical records, passport details, or visa info. But it also includes a fair bit of non-obvious information.

For instance, consider two aspects of SBU described in the US Department of State's rulebook -- the "Foreign Affairs Manual," aka, the FAM (12 FAM 540 "Sensitive But Unclassified Information (SBU), 2013):

1. "Inter or intra-agency communications, including emails, that form part of the

[14] Variations on SBU abound, such as "For Official Use Only" (FOUO) and "Controlled Unclassified Information"

> internal deliberative processes of the U.S. Government, the disclosure of which could harm such processes" as SBU information (12 FAM section 541 "Sensitive But Unclassified Information (SBU)," point b subpoint 9, 2013)
>
> In other words: Work emails? Those could be SBU.
>
> 2. "Before distributing any SBU information, employees must be sure that such distribution is permissible and, when required, specifically authorized" (12 FAM section 543 "Access, Dissemination, and Release," point b, 2013)
>
> In other words: Who's supposed to know if info is SBU? You. And you; and you.

No sharing is safe sharing

This is the crux: emails with other officials can be considered "sensitive"; and figuring out if they are or not is up to each individual official. Or put more simply, even with non-classified information, there are restrictions.

Herein rests the great dilemma of the government official. No one *likes* hoarding information or being excessively secret-like. But it's maddeningly easy to accidently share something that turns out to be a no-no. And the penalty for sharing something that's not supposed to be shared can be pretty stiff.

Here is a hypothetical example of an entirely plausible diplomatic information-sharing fail:

> An intern helpfully offers to post something on Twitter on behalf of the perennially busy ambassador. Assume the ambassador did in fact compose the tweet, but his punishingly packed schedule prevents him from getting to a desktop to complete the tweet process himself. Oh, and there are no cell phones allowed in the buildings (for security purposes), so blackberry-tweeting under the desk isn't an option.
>
> The intern posts the tweet. It's the coolest thing he's ever done. The intern then brags about it on his own Twitter account.
>
> Almost immediately, a reporter notices. A story appears within the hour: "Ambassador X, famous for his 'Twitter diplomacy,' gets interns to tweet for him."
>
> The ambassador's credibility takes a hit. The intern is mortified. And officials who hear about the story may laugh or shake their heads, but also just tweet a little bit less after that.

I picked on an intern, but variations on these things happen to veteran officials, too. Here's an actual example (which, I remind my clear-ers, was already cleared once for my *Foreign Affairs* article, "Social diplomacy, or how diplomats learned to stop worrying and love the tweet" (Wichowski, April 5, 2013):

> On September 11th, 2012, protests erupted across the Arab world in response to an American-made anti-Islamic video posted YouTube. Someone in the Cairo embassy defied recommendations from headquarters in DC and posted a tweet that read: "We firmly reject the actions by those who abuse the universal right of free speech to hurt the religious beliefs of others."
>
> It was an election year. Mitt Romney, attempting to unseat incumbent president Barack Obama, leapt on the tweet, denouncing it as "disgraceful." A popular political blog ran the headline, "US Embassy in Cairo chooses Sep. 11 to apologize for hurt Muslim feelings." Within weeks, the senior official on duty at the embassy that night was removed from his post and recalled to Washington.

I chose Twitter examples because this is a book about digital diplomacy. But the phenomenon of seemingly benign and well-intended words sparking a diplomatic outrage is as old as the modern nation-state. Yet for diplomats dealing with the digital landscape in particular – an environment in which information-sharing, -consuming, -recording are simply more -- the work of knowing what information should be shared and what information should be kept secret is much, much trickier than it used to be.

This chapter focuses on culture. In my 2013 article in *The Atlantic*, "What government can and should learn from hacker culture," I focused on how the structure of government contributes to that culture. Rather than holding onto the structure of government from an age long past -- the legacy of hierarchical "cathedral" like command structure – government would be better served by adopting a flatter, more "bazaar" like structure, similar to the one adopted by the open source programming community.

Whether information-sharing is discouraged because of government's structure or culture, the effects are the same: failure to share information is bad for national security. Kneejerk secrecy scares off officials from sharing information with one another – 9/11, Benghazi, and the Boston Marathon bombing are just a few examples of terrorist attacks that were found to be potentially preventable if government agencies had shared more information with one another. A culture of secrecy is also expensive. According to a May 2013 report by the Congressional Public Interest Declassification Board, each intelligence agency classifies a petabyte of information every 18 months, the storing of which costs over $11 billion dollars (Cox, 2013).

The billboard-sized message here is that the vast majority of diplomatic government officials are already -- without any additional secrecy-culture pressures -- really, really careful with information. Diplomats are profoundly imbued with information-handling awareness and generally exceedingly careful with whether or not to make information public. Ramping up a culture of secrecy doesn't prevent the occasional ill-advised publicizing of sensitive information. It just adds another layer of pressure onto an already highly-pressured work culture. And one of the unfortunate side effects of that pressure is that is teaches them that the safest thing to do is to share as little information as possible; with the public, one's own colleagues; with anyone.

Leakers & their communities

Leakers are government officials. But they also step outside of that role. Once they take the step to leak government secrets, they become something different. The leaker is a highly feared kind of government official, and thus worth spending some time on.

Who leaks? Technically, to qualify as a leaker you have to be a. one of the 1.4 million federal workers with a security clearance, and b. release information you're not supposed to[15]. Can leakers be reduced to job type? Perhaps contractors, like Edward Snowden or the other 485,000 security-cleared contractors,[16] are less loyal than career officials? Or is there some other unifying characteristic that connects them?

If there is a leaker profile, perhaps it's possible to see it by comparing some of the most prominent leakers from the past few decades[17] (Currier, 2013):

Daniel Ellsberg

Senior military analyst. Employed at RAND. PhD, Harvard University. US Marines, '54-57. Leaked documents that showed the US government knew the Vietnam War was unwinnable. They became known as "The Pentagon Papers"

Why he did it

"I felt that as an American citizen, as a responsible citizen, I could no longer cooperate in concealing this information from the American public. I did this clearly at my own jeopardy and I am prepared to answer to all the consequences of this decision." (UPI, 1971)

Samuel Loring Morison

Intelligence analyst. Grandson of Pulitzer-prize winning naval historian Samuel Eliot Morison. Described as a "quiet and scholarly analyst" (Stanley, 1985). Leaked photographs of Soviet ship-building facilities

Why he did it

He's quoted as saying the "public should be aware of what was going on on the other side" (Sunlight Foundation, 2013)

Lawrence Franklin

[15] A caveat: this is an un-nuanced, oversimplified definition. Far more government officials leak than ever get caught. Reporters have suggested that even presidents leak information to the press on occasion (Van Buren, June 12, 2012).

[16] In truth, no one knows exactly how many federal contractors have security clearances. Former Secretary of Defense Robert Gates admitted in an article in the exhaustive *Washington Post* investigation "Top Secret America," "This is a terrible confession. I can't get a number on how many contractors work for the Office of the Secretary of Defense." (Priest & Arkin, July 20, 2010)

[17] With gratitude to ProPublica and the Sunlight Foundation for their thorough spade work on which I expanded here

Senior Middle East analyst for the Defense Department. Father of five. PhD in Asian Studies. Fluent in 7 languages. Gave classified information about Iran to pro-Israel lobbyists working for AIPAC (Johnston, 2006).

Why he did it

According to 2009 interview with *The Forward*, Franklin said he had warned superiors that American soldiers "would return in body bags" from Iraq if policy stayed the way it was. He wanted to "shock [people at the NSC] into pausing and giving another consideration" to current policy (Guttman, 2009).

Chelsea (formerly Bradley) Manning

23 year old soldier stationed in Iraq. Downloaded 1.6 gigabytes of classified diplomatic cables onto a Lady Gaga CD, then transferred the files to a single thumb drive.

Why she did it

"I realized that (in) our efforts to meet the risk posed to us by the enemy, we have forgotten our humanity…When I chose to disclose classified information, I did so out of a love for my country and a sense of duty to others" (Drury, 2013).

Edward Snowden

Computer specialist formerly employed by the CIA and NSA. Dropped out of high school; completed GED certificate; dropped out of community college.

Revealed NSA surveillance practices including PRISM, which involved collecting troves of data on US citizens who were not under any investigation

Why he did it

"My sole motive is to inform the public as to that which is done in their name and that which is done against them" (Leger, 2013).

There are other leak cases that have gone to trial and many more still under investigation. But even just looking at this small subset, one pattern in particular emerges in sharp relief: why they did it. Regardless of their rank -- from senior executive to temporary contractor -- , educational background – from Harvard PhD to high school dropout --, family ties – from father of 5 to bachelor – every one of them said they did it because they believed they were right to do it. And with the exception of Edward Snowden, they remained in country to endure punishment for their actions.[18]

Now we get to the point where all that background on information-sharing and

[18] A month after Snowden fled the US, Daniel Ellsberg (the Pentagon Papers leaker) wrote an op-ed in *The Washington Post* supporting Snowden's decision to leave the country. He wrote, "The country I stayed in was a different America, a long time ago… for the whole two years I was under indictment, I was free to speak to the media… There is no chance that experience could be reproduced today." (Ellsberg, 2013)

information-culture matters. That point is this: leaks don’t just happen. Anyone with a security clearance can leak; almost nobody does. The handful of officials who leaked didn’t do it because they thought they’d get away with it. They didn’t do it because security was too lax. They didn’t do it because government culture encouraged wanton information-sharing behavior.

They did it because they believed their information needed to be shared. They believed it needed to be given to the public. They themselves may not put it in the words of the Brandians or the Pirate Partiers, but through their actions they become advocates for it: they believed the information they had should be free; perhaps even that that information wanted to be free.

~~Soft~~ Difficult power

So far, this chapter has sketched a portrait of the digital landscape. It’s explored how nerve-wracking the digital landscape can be for national security agencies. It’s discussed information-sharing trends in the broader culture, information-sharing influences in government culture, and information-sharing motivations of leakers. There’s one other information-sharing element that demands attention: information-sharing as part of diplomatic power.

A good place to start is the academic battle over “hard” vice “soft” sciences.

In 1987, Pulitzer-prize winning author Jared Diamond wrote an op-ed in *Discover* magazine, commenting on what he called an “intellectual dogfight” over the distinction between “hard science”– the fields of cleanly measureable phenomena such as physics, chemistry, biology, etc; -- and “soft science” – the domain of squishier, more nebulous social sciences like psychology, sociology, anthropology and the like (Diamond, 1987). He argued that “hard scientists” often looked to their “soft” counterparts derisively because the latter’s research subjects seemed so damned fuzzy.

Wrong, he said. Soft sciences are actually harder than the “hard sciences.” “A revolution in the Third World doesn’t fit into a test tube,” Diamond wrote. “You can’t start it and stop it whenever you choose. You can’t control all the variables; perhaps you can’t control any variable.” As such, he argued that the soft sciences would be more aptly called “difficult science.” The “hard sciences” would then become “easy science,” as in easy to measure, control, quantify, test, and replicate.

National security isn’t so different. We call diplomacy “soft power[19],” military might “hard power.” Diplomacy is, like the social sciences, difficult. It’s hard to measure, it’s hard to control -- it’s just plain tricky.

[19] There was an attempt to re-valorize diplomacy by introducing it as “smart power” – defined as enlisting other nations to achieve one’s own national security goals (March/April 2004); but in practice most foreign policy professionals still retain a fairly binary view on state power: diplomacy or defense; soft or hard.

Fortunately, good diplomats know how to master this murk. They're a nation's resident treaders of tricky terrain. Yet to do their job well, they need information. A culture of secrecy makes it harder for diplomats to get information, and harder for diplomats to share information. It makes it harder for diplomats to exchange information with those outside government, and it discourages information-sharing even inside government.

In this way, a culture of secrecy disables not just diplomats, but it disables soft power. It ignores that soft power is actually difficult power. It's complicated power. Like the digital landscape in which it now must operate, diplomatic power is often muddy, fuzzy and squishy. It defies category and certainty. And since the digital landscape will only continue to expand, since dissent and disaffection will spread there before and while and after it erupts in the physical world, and because as more of the world's population finds its way online potential threats tied to the digital landscape will only increase, governments need powerful and empowered diplomats more than ever.

The diplomat's how-to: three steps toward openness

There are actual, tangible, non-job-threatening steps available to diplomats to protect national security AND loosen the reins on secrecy. The final section will explore a few of them.

Step 1: Broaden definitions

Know your audience, and expand your understanding of it. In national security circles, the "audience" includes anyone and everyone who might pose a threat, and anyone and everyone who might be counted as an ally. To find out who's who involves talking to people in government and outside government.

This is perhaps the most important of the three steps. This is because the nation-state's not the only game in town anymore. This chapter argues that the "anyone and everyone" may sort themselves by nation, religion, or ethnic group. But it also includes digital associations where people identify borderlessly with like others. They may do so for lofty purposes, like beliefs, or very humdrum ones, like shared TV show preferences.

While threats to a nation's physical security may still involve in-person action, like the Boston Marathon bombers dropping off an explosives-filled backpack at the finish line, threats to physical security may also involve a whole lot of behind-the-digital-scene activity. Diplomats must be aware of who's out there, regardless of whether they identify by nation or beliefs like information-wants-to-be-free.

An example, featuring the activist group Anonymous, illustrates this:

> On July 3, 2011 in San Francisco, California, 45-year old Charles Blair Hill, a homeless man, drunk and reportedly making threatening gestures, was shot and killed by police officers working for San Francisco's "Bay Area Transit System,"

> better known as BART. Immediately after the killing, angry citizens used social media to coordinate mass protests in real-time, forcing the transit system to a halt (Fagan, 2011).
>
> After the protest in San Francisco, the activist group Anonymous stepped in online. Anonymous self-describes as an "internet gathering" that "operates on ideas rather than directives." They're totally decentralized. No one really knows how big they are, but they're a force of some magnitude: they've been linked with Wikileaks, the Occupy movement, and the Arab Spring. In 2012, *TIME* magazine listed Anonymous on its "World's 100 Most Influential People" list (Norton, 2012).
>
> Anonymous orchestrated a second protest: OpBART, a flash mob that would assemble via on-the-fly cell phone coordination. But authorities at BART got tipped off about it before the protest had a chance to take place. To prevent the real-time flash mob, authorities shut down cell service throughout the stations (Fagan, 2011).
>
> Citizens did not like this[20]. News stories about the service shutdown spread through social media networks around the country, prompting nation-wide outrage. The ACLU sent a letter to the BART chief of police, denouncing BART as the "first known government agency in the United States to block cell service in order to disrupt a political protest" (Soltani & Schlosser, 2011). The Federal Communications Commission launched an investigation to determine the legality of BART's actions[21].

It might seem like the scenario described here is a bad example for a chapter for foreign policy professionals – this happened on US soil. But Anonymous, and movements like it, are not domestic; they're international. As internet and cell phone reach expands and the rest of the global population get online, borderless associations will only grow.

This example also shows that the same categories of person can be both a threat to

[20] Citizens didn't like it in the Ukraine, either, when in 2014 now-ousted President Yanukovich forced cell phone providers in Kiev to tag protestors, sending the text: "Dear subscriber, you are registered as a participant in a mass disturbance" (Murphy, 2014).

20

[21] Under Standard Operating Procedure 303 (SOP 303) the government is permitted to shut down cell phone service in certain circumstances. The SOP 303 (Emergency Wireless Protocols) detail shutdown and restoration procedures in the event of a "national crisis." The FCC investigation was to determine if BART was operating under such conditions. As of April 2013, the FCC inquiry was still open (EPIC, 2013).

[21]To force a decision, internet advocacy group the Electronic Privacy Information Center (EPIC) sued the Department of Homeland Security (DHS) under the Freedom of Information Act. According to EPIC, "How do we know that DHS is following the First Amendment or considering these important interests adequately? DHS has said nothing about its deactivation policy apart from a single paragraph in an old report." On November 12, 2013, the federal judge presiding over EPIC's case ordered DHS to disclose the details of their deactivation policy (http://epic.org/foia/EPICvDHS-SOP303-Order.pdf). At the time of this writing, the DHS had not yet done so, as they were within their 60-day window to appeal.

national security or act as ally in protecting it. For instance, citizens who physically disrupted subway service may be seen as a threat to public safety, but those who protested against the cell-phone shutdown may be seen as advocates for defending freedom of speech. The authorities could also be seen as both and threat and ally: police officers who use excessive force are threats to citizens, but police officers who halt transportation-disrupting protests are allies in protecting them.

Diplomacy is trickier than ever; let's not pretend otherwise. Expand your awareness of who's out there. To do so, diplomats must resist retreating into the comfort of secrecy. Talk to people. Know what's going on online, as well as in country.

Step 2: Engagement

Diplomats can't avoid social media. They must stake a flag in the public online domain. Most diplomats get this by now – official Twitter and Facebook accounts are by 2014 accepted practice. But while lots of diplomats use social media, only a handful of them use it really well.

To use it well, you have to post more than anodyne press releases. People don't care about policy guidance; they care about other people -- especially powerful people who say something interesting and real. So say something real. Be careful, but don't let care keep you from saying anything. Reflexive secrecy prevents realness.

In an article I wrote for *Foreign Affairs*, "Social diplomacy: how diplomats learned to stop worrying and love the tweet," I describe some of good diplomatic Twitter practices in detail (2013). To summarize here, I argue that 140 characters at a time, diplomats can make statements; condemn, call out, exhort, urge, shine a light. One tweet may not seem to matter; but a record of tweets – and their retweets and their retweets – can add up quickly.

The US ambassador to the United Nations and diplomatic Twitter devotee Samantha Power often says that when approaching foreign policy problems to "look at every tool in the toolbox[22]." When she wrote this in *A Problem from Hell* she was talking about preventing genocide. Twitter didn't exist then; "digital diplomacy" wasn't one of the tools. But the spirit of the message applies. Social media is a powerful tool. Thousands of ambassadors, foreign ministers, presidents and kings are starting to get that. Diplomats can help them by showing foreign policy leadership how to not just use social media tools, but how to use them well.

Step 3: Reduce hypocrisy

Assume everything – everything -- will be found out. It won't, but assume it will. Align

[22] Disclaimer: I work in her press office. I feel reflexively compelled to note her Twitter handle is @AmbassadorPower

what you do with what you say you do. Some people won't like some policy, but no people like hypocrisy.

In the intriguing essay, "The end of hypocrisy: American foreign policy in the age of leaks," political scientists Henry Farrell and Martha Finnemore (2014) suggest that damage from leaks comes not so much from any specific revelation, but because they "undermine Washington's ability to act hypocritically and get away with it." They argue that hypocrisy has been especially damaging to America's soft power precisely because it's America: a nation that repeatedly seeks legitimacy through its ideals, like rule of law, democracy, and free trade. If government actions undermine the law, democracy or free trade, the nation's legitimacy is undermined too.

In other words, hypocrisy damages national security, because it calls into question whether the ideals on which a nation is built actually matter. And if people online are indeed increasingly allying themselves with borderless collectives centered on beliefs, then bolstering the ideals of a country as something to believe *in* is more important than ever.

Closing thoughts

Digital information expands the reach of human capacity – to connect, to ally, to inform others and be informed by – and it does it at an accelerating pace. Like outer space, the digital universe expands.

To step back and consider this expanding, accelerating plane can be overwhelming, and terrifying, and awesome; it's a little like space in this way too. Thus, it feels only fitting to conclude the chapter with a quotation from someone who's been there.

Describing what it was like to see the earth from the moon, Apollo 13 astronaut Edgar Mitchell said:

> "You develop an instant global consciousness, a people orientation, an intense dissatisfaction with the state of the world, and a compulsion to do something about it.
>
> From out there on the moon, international politics look so petty. You want to grab a politician by the scruff of the neck and drag him a quarter of a million miles out and say, 'Look at that, you son of a bitch."

A people orientation, an intense dissatisfaction with the state of the world, and a compulsion to do something about it: sounds a lot like diplomacy.

References

(1969, *The Whole Earth Catalogue)*

11 'leakers' charged with espionage.(July 12, 2013, *Churnalism: The Sunlight Foundation,*

12 fam 540 sensitive but unclassified information (sbu) (03-05-2013). No. CT:DS-190)Office of Origin: DS/SI/IS.

1971 year in review: The pentagon papers.(1971, *Upi,*

Anderson, B. (2006). *Imagined communities: Reflections on the origin and spread of nationalism* verso.

Bennett, S. (2013, Social media overload – how much information do we process each day? *Mediabistro,*

Clark-Dickson, P. (April 29, 2013,). OTT messaging traffic will be twice the volume of P2P SMS traffic by end-2013. Message posted to http://blogs.informatandm.com/12861/news-release-ott-messaging-traffic-will-be-twice-the-volume-of-p2p-sms-traffic-by-end-2013/

Cox, R. (May 30, 2013, Shaheen to obama: 'over-classification' in government costs taxpayers money

Currier, C. (July 30, 2013, Charting obama's crackdown on national security leaks. *ProPublica,*

Diamond, J. (August 1987, Soft sciences are often harder than hard sciences *Discover.*

Ellsberg, D. (July 7, 2013, Snowden made the right call when he fled the U.S. *The Washington Post.*

Executive Order 12958-Classified National Security Information, as Amended, (March 28, 2003).

Fang, I. E. (1997). *A history of mass communication: Six information revolution*s Taylor & Francis.

Farber, D. (May 13, 2013, Google search scratches its brain 500 million times a day. *CNET.*

Fitchard, K. (November 11, 2013, Ericsson: Global smartphone penetration will reach 60% in 2019. *Gigaom.*

Garfield, S. (2013). *To the letter: A celebration of the lost art of letter writin*g. New York: Gotham Books.

Google annual search statistics., Februrary 12, 2014, from http://www.statisticbrain.com/google-searches/

Granger, L. (December 30, 2013,). Billions of users and tweets per minute: Social media in 2013 by the numbers. Retrieved from http://memeburn.com/2013/12/billions-of-users-and-tweets-per-minute-social-media-in-2013-by-the-numbers/

Greenwald, G. (June 9, 2013). "NSA whistleblower Edward Snowden: I don't want to live in a society that does these sort of things' – video." *The Guardian* http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video

Internet world stats. January 14, 2014. Retrieved from www.internetworldstats.com/stats.htm

Johnston, D. (January 20, 2006, Pentagon analyst gets 12 years for disclosing data*. The New York Times.*

Leger, D. (June 9, 2013, NSA contractor: 'I know I have done nothing wrong'. *USA Today.*

Leonard, A. (January 7, 2014) Evgeny Morozov's New Yorker put-down of the maker movement misses the point*. Salon.*

Mazzone, J., & Rehman, S. (April 2011). *The household diary study: Mail use and attitudes* FY2011. The United States Postal Service.

Morozov, E. (January 13, 2014). Making it: Pick up a spot welder and join the revolution. *The New Yorker.*

Norton, Q. (July 3, 2012) How anonymous picks targets, launches attacks, and takes powerful organizations down*. Wired.*

Nossel, S. (March/April 2004). Smart power. *Foreign Affairs.*

Pfanner, E. (April 17, 2009). Four convicted in sweden in internet piracy case, *The New York Times.*

Pirate bay continues to expand despite mounting anti-piracy movement. (December 31, 2013, *RT News.*

Priest, D., & Arkin, W. (July 20, 2010). National security, inc. *The Washington Post.*

Radicati, S., & Buckley, T. (October 2012). *eDiscovery market, 2012-2016 – Executive Summar*y. London: The Radicati Group, Inc.

Sagar, R. (2013). *Secrets and leaks: The dilemma of state secrec*y. Princeton, NJ: Princeton University Press.

Schmid, R. U.S. postal service survey reveals personal letters at record low. *The Huffington Post.*

Smith, A. (September 19, 2011). *Americans and text messagin*g. Pew Internet & American Life Project.

Stanley, A. (October 15, 1985). Spy vs. spy saga. *TIME.*

Stewart Brand, Kevin Kelly, George Dyson: A Edge conversation in Munich.(February 7, 2011, *Edge@dld,*

Swartz, O. (April 17, 2009). The Pirate Bay guilty; jail for file-sharing foursome. *Wired.*

Van Buren, P. (June 12, 2012), Obama's war on whistleblowers. *Mother Jones.*

Varadarajan, T. (November 28, 2010). The fallout from Wikileaks’ latest exposure. *The Daily Beast*.

Wichowski, A. (April 5, 2013). Social diplomacy or how diplomats learned to stop worrying and love the tweet. *Foreign Affairs.*

Wichowski, A. (October 25, 2013, What government can and should learn from hacker culture. *The Atlantic.*

YouTube: Statistics. Retrieved on January 7, 2014 from http://www.youtube.com/yt/press/statistics.html