POWER OVER INFORMATION FLOW

Dorothy E. Denning
November 19, 2009

Information flows through a global environment characterized by conflict and competition. One party wants a flow to occur; another wants to block it. To illustrate: users want to freely exchange information, while governments and businesses seek to block information harmful to their interests. Spies try to infiltrate the networks of their adversaries and competitors to gather intelligence, while their targets employ security mechanisms to prevent network exploitation and attack. Hackers and identity thieves send e-mails loaded with viruses and other forms of malicious software, while users employ anti-viral tools to block the same.

Conflicts over information flow are at the heart of information operations and warfare, to include cyber warfare, cyber crime, and cyber conflict in general. One party sends packets or streams of information that aim to attack, exploit, or influence a target, while the opponent employs measures to stop the flows. The cyber assault against Estonian in 2007, for example, was launched by patriotic Russian hackers who were incensed by the relocation of a Soviet-era war memorial in Estonia's capital, Tallinn. To express their outrage, they flooded select Estonian websites with internet packets, exploiting at least one "botnet" of compromised computers to create a massive amount of traffic. Their distributed denial-of-service (DDoS) attack shut down the sites until the Estonians could effectively block the traffic and the hackers backed off. Russian hackers launched similar attacks against Georgian websites in 2008, this time in conjunction with a military confrontation between Russia and Georgia over South Ossetia.

Not all information-related conflicts center on cyber attacks. Following the 2009 presidential election in Iran, for example, protestors used various cyber media including Twitter, Facebook, YouTube, and text messaging to distribute information and videos about the protests. In response, the Iranian government took steps to block access to certain websites and media. The government's efforts were only partially effective, however, as Iranians shared information and tools for circumventing the censors. Some of the protestors also launched a DDoS attack against President Ahmadinejad's website, but this was short-lived and played a minor role in the overall conflict.

This paper examines the global flow of information in terms of a power struggle between efforts to cause flows and efforts to block them. It analyzes the nature of this power, how it is exercised, and the objectives served. Although a variety of information media are considered, emphasis is placed on flows enabled by computer networks, including the internet and mobile phone networks. Whereas information flows were at one time dominated by human interactions within small localities, today they are facilitated by global networks of hardware and software systems. The software itself is data, allowing it to flow like other information. But unlike other forms of information, which are effectively inert, software causes things to happen, including information flows. Spyware,

for example, captures data on one computer and transmits it to another; computer worms spread their damaging code to other vulnerable hosts.

In viewing the global flow of information as a power struggle, the paper does not mean to imply a lack of cooperation and collaboration in the information environment. Indeed, people frequently cooperate to share information and promote flows, as well as to stop them. The world's largest encyclopedia, Wikipedia, is the product of widespread collaboration on the internet. But even there, conflicts are common over specific content, as users edit and delete material to serve their interests.

After examining the power of flow and the power of blockage, the paper looks at the characteristics and challenges of flows that are covert in nature. It then examines how laws and regulations support blockage power and, to a lesser extent, flow power. With this background, the paper considers the issue of information control, and whether this is even possible. Finally, it turns to the question of what power over information flow means in terms of influence. Ultimately, it is not the ability to control flows that matter as much as the ability to influence decisions and actions.

Flow Power

Information flows arise when information is transmitted from a source (or sender) to a destination (or receiver) over some channel. The source can be a human; a device such as a computer, sensor, or broadcast station; or some combination, as when a user sends an e-mail message from a laptop or places a call from a mobile phone. Similarly, the destination can be a human, device, or both. The information channel may be provided or mediated by third parties, including communication service providers and governments. Further, the channel itself may be the source or target of additional flows, as when it is wiretapped.

Flow power is the ability to cause a flow of particular information from a given source to a given destination within a specified time. Time is an important element, because information can become stale and irrelevant.

Flow power can reside at the source, destination, or channel. At the source, power is characterized by an ability to *push* information to the destination. The means vary and include sending an e-mail, text, or instant message; talking in person or on the phone; transmitting a fax; broadcasting a television or radio program; and uploading information to a website or file directory.

Power at the destination is characterized by an ability to *pull* information from the source. A principal means is downloading information from a website or file server.

Many, perhaps most, information flows result from a combination of push and pull. Radio and television broadcasters push their programming onto the airwaves; viewers pull the ones they desire by tuning their receivers to the specified channels. Owners of websites push information onto their sites; interested users visit the sites and pull the

information they want; they may also push new information onto the site by filling in a form or adding comments to a discussion thread. Even e-mail, which is predominantly a form of push, requires some pull from the recipient, namely to select, open, and read a message in the inbox. The result is that flow power may be shared by senders and receivers, with neither party being in full control of the flow. Still, the balance of power may not be even. E-mail and postal mail seem to favor senders, as illustrated by junk mail.

In some cases, the sender or receiver can execute a flow without help from the other party, or at least a human party. For example, pop-up ads are essentially pushed onto a user's computer, although facilitated by software running on the user's machine. Fax is another example which puts virtually all of the power in the hands of the sender. As an example where the receiver of information has the power, consider a hacker who breaks into another computer system. The hacker can pull information from the compromised machine without the owner's cooperation or consent, assisted only by software on the computer (possibly even pushed there by the hacker).

Third parties who provide or control the information channels also have power over information flows. These include internet service providers, and the owners and operators of network routers and name servers. E-mail and web traffic cannot flow without this basic infrastructure. In addition, much of what people access on the web is mediated through search engines, which control the order of entries in "hit" lists and which sites on the web are indexed. The authors of blogs and other types of web pages also facilitate flows by linking to other pages.

Receivers of information can serve as intermediaries for additional flows by forwarding the information to others, thereby facilitating flows from the originating source to downstream recipients. Indeed, information often flows through social networks via e-mail and other channels, reaching people not even known to the originator. In the process, intermediaries serve as brokers or gatekeepers to further flows.

In general, flow power is increasing across the board. One reason is that the volume of information is increasing, so there is considerably more information to push and pull. But technology has played an even larger role, reducing human effort at both the sending and receiving ends, and reducing transmission times and costs. Software performs many tasks that once required considerable human effort, such as sending mass mailings and regular news updates, and managing distribution lists. Today's messaging environment has made it virtually effortless to send new and forwarded information across the globe in practically no time and at practically no cost. The web, together with powerful search engines that comb it, has become an enormous library and marketplace, empowering those who want to find and acquire information as well as those who want to publish and disseminate it. The benefits are enormous, but they are partially offset by numerous problems: spam, pop-up ads, computer viruses, hackers, and so forth.

Blockage Power

Blockage power is the ability to prevent particular information from flowing from a given source to a given destination. It is the opposite of flow power and serves to undermine it by denying, degrading, and disrupting information flow.

As a rule, blockage power is selective. The goal is not to prevent all information flow, only those that deemed harmful. Blockage power is directed at a range of information, including spam; malicious software such as computer viruses, worms, Trojan horses, and spyware; sensitive information sought by spies; intellectual property transmitted in violation of copyrights; information contraband such as child pornography; and information censored by governments.

Like flow power, blockage power can be exercised at the source or destination, or by third parties along the way. At the source, it takes the form of security measures, including access controls, filters, encryption, and digital rights management. Access controls deny unauthorized persons the ability to transmit information from the source. They typically depend on a system of user identification and authentication, such as user names and passwords. However, they can be based on other factors such as location. Jihadist websites, for example, have been known to prohibit access to visitors from certain countries. Filters, including firewalls and anti-viral tools, serve to block certain information from leaving the source, including packets and messages with malicious code. Encryption protects data both in storage and in transit. Even if the bits flow, the information conveyed by them will be inaccessible to those without the key or the means to crack the code. Digital rights management (DRM) uses a combination of access control and encryption to protect intellectual property from flowing in ways that violate a licensing agreement.

Security is also essential to block flows at the receiving end. Access controls deny unauthorized persons the ability to deposit information at the destination. Filters block incoming information deemed harmful, including packets associated with computer intrusions. They stop malicious software and spam that arrives via messaging systems or web browsing.

Intermediaries also have the power to block flows. Infrastructure operators can filter out spam, malicious code, and information that violates policies and laws. Web hosting services in the United States and elsewhere have taken down thousands of websites containing child pornography, pirated software and music, and scams. They have also removed jihadist websites supporting terrorists. In China, where information is heavily censored, internet service providers are required to filter out and remove banned information. Information entering the country is filtered at border routers implementing China's "great firewall."

Third parties can block flows even if they do not own or control the infrastructure. For example, they can keep information from flowing in or out of a website by bombarding the server with worthless traffic, as was done with the Estonian and Georgian cyber

attacks. Even if the channels are not fully blocked, these denial-of-service attacks can substantially degrade legitimate flows. Such attacks have driven some e-commerce sites and internet service providers out of business, because they could not sustain the losses. Others have given in to extortionists, paying perpetrators to stop their attacks.

Unscrupulous businesses have also engaged in “click fraud” in order to get their competitor’s click-through ads off the internet. For example, by repetitively clicking on prepaid ads that are limited to so many clicks, they can drive the clicks up to the limit, whereupon the ads are removed.

Just as information technology has increased flow power, it has increased the power to block those flows. Information security and content filtering tools, for example, continue to improve, making it possible to block traffic that at one time flowed freely. As bad as spam is, at least it is amenable to blockage, whereas postal junk mail is not. However, considering the rate of increase in information flow, it is not clear that advances in blockage power have kept up with flow power. Part of the reason is that improvements in blockage motivate those who wish to move information to find new ways of doing so. Often, the new methods are covert and distributed, making them much harder to observe and stop.

Covert Power

Covert power is a form of flow power where the information flow is hidden. The objective is to conceal the source, destination, or content from an adversary who might observe or obstruct the flow.

A wiretap or other type of hidden communication intercept is an example of a covert flow where a copy of the intercepted message stream flows secretly to a hidden receiver. However, although the communicants may not know their messages are being read or heard, they can effectively block the covert flow by encrypting their communications, as noted earlier.

Most computer attacks involve covert flows. Hackers, for example, secretly plant malicious software, including spyware and hacking tools, on vulnerable machines. The software allows the hackers to secretly exfiltrate sensitive information from the systems. In addition, the compromised machines may be employed in botnets that send out spam and launch DDoS attacks, all without their owners knowing. Likewise, computer viruses and worms spread secretly from one machine to another without the owners even realizing that their machines have been infected.

Some covert flows circumvent security controls at a destination by pretending to come from a trusted source. Packets get through firewalls with fake IP source addresses, and malicious e-mail arrives with spoofed headers. Users unwittingly open e-mail attachments and click on links to malicious websites thinking the e-mail came from their bank or other trusted party. In a typical “phishing” scenario, the user is duped into typing in personal information such as a username and password or social security number.

Initiators of flows can also hijack channels in order to take over a network connection or broadcast medium. Israel, for example, hijacked live broadcasts from Hezballah's Al-Manar television station in order to supplant the station's regular programming with its own messages.

In some cases, the source and destination of a flow collaborate in order to hide a flow from third parties such as wiretappers. An example is the use of steganography, which attempts to hide the transmission of information. By hiding the message within a cover medium such as an image or video, the communicants can conceal the flow of the message from third party observers. However, a third party may observe the flow of the cover message and thereby learn that at least something is being communicated. Encryption is similar, but in this case the message is hidden by scrambling the bits rather than trying to conceal its transmission.

Third parties can facilitate covert flows. Proxy servers, for example, allow users to browse the web while concealing their IP address from a visited website, and the website's IP address from intermediaries (e.g., governments) watching what flows in and out of the user's computer. They provide one means whereby users in China, Iran, and other countries that censor the Internet can get around the filters that prohibit access to certain foreign sites. Banned information can also slip past the filters of these countries through the use of encryption and steganography. Software tools have been developed to explicitly support these covert flows.

Laws and Regulations

The preceding discussion illustrates how technology enhances both the power of information flow and the power of blockage. This power is also strengthened through laws and regulations. Those that support the rights of free expression and access to information strengthen the power of flow, while those that restrict those rights strengthen the power of blockage.

Most if not all governments have regulatory authority over their information environment. Authoritarian governments generally restrict more information than democracies, but even democracies prohibit certain types of information such as child pornography, defamatory speech, fraudulent advertising, and speech that incites violence. In addition, governments have laws protecting classified information from disclosure and intellectual property from piracy and theft. When these laws and regulations are broken, infrastructure owners are entitled to block offending information flows. They can take down websites or remove files from them, block broadcasts and individual messages, and deny access to perpetrators. At the same time, free speech laws ensure that public providers cannot block information flows just because they find them offensive. In addition, the Freedom of Information Act (FOIA) and corporate disclosure laws ensure that government agencies and corporations release certain information even when they would prefer to withhold it.

Regulations do not provide absolute power over information flows, as laws can be violated and information can flow covertly. Further, enforcement across borders can be difficult. Information prohibited in one country may not be in another, and monitoring information flows over borders is difficult at best. Citizens of a country where information is prohibited may be able to acquire it from foreign sources by covert means, as noted earlier.

Still, laws and regulations matter. Most internet service providers in China abide by the regulations to censor, lest they risk heavy penalties or closure. This is equally true of western companies operating within China, leading to criticisms of Google, Cisco, and others for supporting the censors instead of demanding free speech. In addition, most Chinese accept the legal regime and self-censor. Relatively few flagrantly violate the law, and many that do end up in prison.

Although intellectual property laws have certainly not prevented the flow of software, music, and other files in violation of copyrights, they have arguably reduced their flow. Lawsuits against businesses found to have unlicensed software motivated companies to make sure the software on their computers was licensed. Similarly, those against Napster and other services that promoted unfettered music sharing led to the launch of new services that better support the protection of intellectual property, while enabling its flow. Had these and lawsuits against individual violators not been filed, copyrights might be meaningless in today's information environment.

Control

Control over the information environment is usually regarded as the ability to prevent certain flows, including downstream flows following the limited release of information. The general consensus is that these flows cannot be controlled. Once information is out there, especially on the internet, it cannot be retracted or restricted to particular parties. It can go anywhere, assisted by covert means or even overtly. Moreover, anything can be put on the internet, in defiance of government and corporate censors.

This paper takes the view that the issue of control is more nuanced. Although the ability to block flows is never complete, steps can be taken to considerably reduce the likelihood or extent of particular flows. These steps can draw upon both technology and the law. In China, the information environment is strongly affected by laws and regulations governing users and service providers, by the products that block and filter flows at the border routers and internally, by the thousands of cybercops who enforce the laws, and by the severe penalties imposed on violators. Chinese users can circumvent the filters using encryption and steganography, but most do not bother.

Information placed on the internet may seem impossible to take back, yet it happens all the time. News sites remove stories from public view, organizations pull documents, and entire websites disappear. In some cases, the information may still be on the net, but hidden on a page that is password controlled or not seen by search engines. Unless the information has been copied to a public website that is scanned and indexed by major

search engines, it will be as good as gone, as far as most users concerned. That the information may exist somewhere will be of little value. The internet archive (www.archive.org) is an ambitious attempt to keep a record of information posted on the internet, but it is far from complete, and information has been removed from there as well.

Still, there are many situations where people lose control over their information. Internet users give their personal information to a website, only to learn that it has been compromised by hackers or sold to a third party. They find out that sensitive information sent in a private e-mail was forwarded to others or posted on a website. They discover that their search queries are logged and potentially available to the government. They find out that a software product installed on their computer has hidden spyware, which has been sending information from their machine to the vendor's. Government officials post redacted documents on their websites, only to learn that the "deleted" information was inadvertently exposed and published on a site outside government control. Information security mechanisms protect against some of these flows, but not all.

In general, it is easier to control information the closer it is to the source. If the photos taken at Abu Ghraib had never been taken or entered the public domain, where they quickly spread around the world, the impact would have been far less. Better still, had the prisoners never been abused, there would have been no story of mistreatment to report in the first place. Even if we cannot completely control the downstream flow of information, we can control our actions, which in turn affect the information generated about us and disseminated to other parties. However, we are still not in complete control, as people can concoct and propagate conspiracy stories and other falsehoods. These stories will co-exist with accurate ones in a sea of information where perception can matter more than truth.

Overall, governments have greater control over the information environment than other entities, because of their ability to censor information within their borders under national laws, however limited that power may be. But organizations are not powerless, as they can fire their own personnel for accessing or posting inappropriate information, and they can sue those who steal their intellectual property.

In addition to blocking information, governments and other entities can attempt to shape the information environment through information flows. They can flood the information environment with carefully crafted messages, submit stories to the press faster than their opponents, and post messages on venues that draw large audiences. Indeed, it may be more effective to post information on a popular website than on one that is rarely visited but under the publisher's control. Chinese authorities, operating undercover, reportedly post commentaries defending the government on Internet discussion sites to counter negative comments on those sites, finding this to be more effective than posting to official government sites.

Influence

Ultimately, one's goal may go beyond simply causing or blocking flows, or even controlling the information environment. It may be influencing the opinions, decisions and actions of target audiences. Governments are interested in promoting their national and international agendas; political parties seek votes for their candidates; and businesses want consumers to buy their products.

For information to influence people, it must first reach them. This can be easier said than done. Simply publishing information on a website or broadcasting it over the airwaves does not guarantee it will get to a target audience. The audience may never visit the site or tune their stations to the desired programs. As noted above, posting information to already popular websites and other media can help. In the Arab world, one can reach a much larger audience through al-Jazeera than CNN.

Sending information directly via e-mail or other messaging systems is also problematic, as the messages may be viewed as spam and discarded. These systems generally work best when the receivers knows the senders and are favorably disposed toward them or have asked for information from them, for example, by subscribing to an e-mail newsletter or following someone on Twitter. Another strategy is to relay the message through a trusted relationship; instead of contacting the target directly, the message is sent to a trusted friend or colleague of the target. Internet services such as LinkedIn give users the ability to construct, manage, and use trust networks to reach people they do not otherwise know.

Assuming a message has reached its target, how the target responds will be a function of the message's perceived credibility; the target's psychology, past experiences, social communities, and culture; the target's relationship to and views of the source of the information; and the context in which the message is received. A message that appeals to a government's own citizens might be found repugnant to a foreign audience.

The ability to influence another party can be based on different types of power relationships. John French and Bertram Raven identified five in their seminal paper "The Bases of Social Power" (*Studies in Social Power*, 1959): reward, coercive, legitimate, expert, and referent.

With reward power, influence is achieved by mediating rewards to the target of influence, where the granting of rewards is contingent on the target taking a desired action (or inaction). Con artists exploit reward power by promising benefits that are never delivered. With the Nigerian 409 scams, victims believe they will receive millions of dollars after putting up a few thousand; instead, they find they are duped. Enough people fall for such scams that a considerable portion of the global e-mail traffic contains fraudulent messages.

With coercive power, influence is achieved through threats or acts of punishment.

By serving lawsuits against file sharing services that facilitated music sharing in violation of copyrights, the music industry influenced the development and deployment of products and services that support copyrights. Extortionists have also used coercive power, threatening to disclose secrets acquired by hacking or to launch a DDoS attack against a critical website unless the victim pays.

Legitimate power refers to the power that comes from the authority vested in roles and social norms. The target of influence accepts that the source has the authority to prescribe certain actions. As noted earlier, most Internet users in China accept the rulings by their government about posting certain types of information on the Internet. Similarly, employees accept certain restrictions imposed by their organizations on internet use. In many cases such as these, the legitimate power is also backed up with coercive power, for example, the threat of being fined, imprisoned, or fired.

With expert power, one's influence on another party is based on knowledge and expertise that has value to the other party. The information supplied by experts is generally more likely to receive widespread distribution and be acted upon by recipients than information from non-experts.

Referent power is one of the strongest forms of social power. It is based on a feeling of attraction to and identification with the influencer. The target of referent power will take actions to please, imitate, or support the source, for example, by buying a product or donating to a charity promoted by a celebrity. The source may not even be aware of the power held over the target. Referent power is similar to the soft power described by Joseph Nye in his book by that title. Like the other forms of social power, people with referent power have an advantage when it comes to reaching and influencing others.

Intermediaries also play a role in influence. Consumers consult product ratings and reviews before making purchasing decisions; voters talk with family and friends before filling in their ballots; and government leaders examine intelligence reports before making certain decisions. In some cases, the value of intermediaries can be subverted. For example, book authors can improve their ratings on Amazon.com by supplying anonymous five-star reviews of their own books. Similarly, they can lower the ratings of competing books by supplying anonymous one-star reviews of those books. By submitting numerous reviews from phony reviewers, both scores can be further affected.

Conclusions

The global flow of information is competitive, with the power of flow frequently bumping up against the power of blockage. While no player has complete control over the information environment, each has limited power to cause or support certain flows and block others. However, there is a constant tension between the power of flow and the power of blockage. Channels that seem to be blocked may be circumvented through covert flows; yet, at the same time, flows that seem impossible to block technically may be sharply reduced through laws and regulations.

The competition between flow power and blockage power is manifest in both domestic and international conflicts. In addition, it has given rise to several information-related conflicts, including the free flow of intellectual property vs. copyright protection, free speech vs. government censorship, spam vs. e-mail control, hacking and malicious software vs. security and privacy, and government and corporate surveillance vs. privacy. None of these have or are likely to have clear winners and losers, as technology continually advances to support new means of flow and new means of blockage. At the same time, the legal environment adapts to better empower certain actors.

In at least some of these conflicts, the ultimate question is not who wins the flow wars, but who wins at influence. Which companies succeed in the market? Which governments realize their policy agendas? Do individuals retain their civil liberties? Still, the global flow of information plays a critical role in determining influence, and is fundamental to it. As long as there are competing agendas, there will be power struggles over the information environment.