Abstract

LeaksWiki is a wiki about leaking organizations, the tools and methods used in leaking, and how leaking can improve in the future. The goal of LeaksWiki is to make leaking safer, easier, and more effective through a transparent understanding of leaking organizations. Both LeaksWiki and this paper present a framework of leaking ideologies from radical transparency to selective release. They further argue that while the leaking process may differ based on leaking ideology, all organizations follow a general leaking procedure. Five case studies of leaking organizations are presented and discussed within the context of this process. The paper concludes that while the current approach to leaking works for some releases, leaking still can be made more accessible through transparency and leaking organizations still face many challenges and have room for improvement. Most of the text that follows is adapted from LeaksWiki articles on leakswiki.org.
I. Introduction

Transparency is changing. Leaking websites and organizations are increasingly widespread. In large part, this rise of leaking organizations is likely due to the controversies around WikiLeaks. Leaking organizations are noteworthy because they separate the source from the release of the document or information and thus significantly alter the process of leaking, disclosure, and whistleblowing (Greenberg, 2012). This separation has a few important implications. First, the separation of the source from the document release makes the leaking process safer for the source or whistleblower. Anonymous submission systems give the source anonymity in the initial transmission of documents and the disconnection of the source from the release makes the source less traceable. Second, the process becomes easier for the source to release any documents or more documents (Hood, 2012). The intermediary leaking organization can study the documents in-depth, prepare them for release, work with media partners, and perhaps advocate for correction of a wrongdoing. Third, there is now a middleman in the process, the leaking organization (Chen, 2011). However, this can be both a benefit and a detriment. The leaking organization can be an additional security risk to the source and innocent people mentioned in the leaked documents, but it is also a body often (but not always) independent of government agencies, companies, and mainstream media institutions. The independence of the leaking organization may sometimes make it easier for them to serve as an additional check on traditional institutions (Lovink and Riemens, 2010). Fourth, there is now a group of people tasked primarily with determining how to make a leak successful and broadly defining what a successful release of leaked documents means.
Leaking organizations are enabled by technology, which explains why they are a fairly new phenomenon (Caryl, 2011). The anonymity of the source requires additional layers of separation between the leaking website and the source. Usually, these take the form of the Internet, encryption, tools like Tor, and other security technologies (Greenberg, 2012). Technology also makes the leak more feasible and enables large leaks. Greenberg refers to these large leaks as 'megaleaks'. Large releases, like the Pentagon Papers, were possible before the Internet and the rise of leaking organizations but Megaleaks are only feasible because of the existence of computers, increasing information storage capacity, the ability for many people to view documents online, and faster uploads and downloads (Greenberg, 2012). Leaking organizations further enable megaleaks by examining and preparing large leaks for release. They are a technology-enabled way of outsourcing parts of the whistleblowing or disclosure process. Some leaking organizations even outsource the process by using crowd sourcing in document processing (Hood, 2011). Additionally, the people involved in leaking organizations and those reading the documents after release are only able to fully understand megaleaks because the Internet makes more information available to non-experts than ever before (Noveck, 2008). Leaking organizations are a way of taking power away from these experts and institutions who would have normally handled documents that are now leaked.

Unfortunately, leaking suffers from a lack of transparency. Many leaking organizations do not discuss the tools and procedures they use to internally process leaks, despite leak processing being their primary purpose (Lovink and Riemens, 2010).

To better understand leaking organizations and their processes and methods, this paper attempts to answer the following four questions about leaking organizations.
1. How does leak processing fit within the goals and philosophies of leaking organizations?

2. What do leaking organizations do with documents to prepare them for release (leak processing)? What specific tools and methods are used in leak processing?

3. How are the processes of leaking organizations different? Do all leaking organizations have some steps in common?

4. How can the current approaches to leak processing be improved?

To investigate these questions, I first suggest a theory of transparency ideologies. Second, I lay out a general framework for the leaking process that all leaking organizations follow. Third, I present case studies that explore leaking ideologies, processes, and outcomes for five organizations within the context of my leaking process framework. Fourth, I use my leaking process framework to discuss the common approaches and primary differences between leaking organizations. Fifth, I discuss how the current approaches to leak processing may be improved.

II. Spectrum of Transparency Ideologies

Leaking organizations can be powerful forces of social change. The ideal type of change varies based on the ideology of the specific leaking organization. Some organizations hope to correct specific wrongdoings. Others want to publicize certain information. Some seek to encourage a general culture of transparency. The specific ideology of a leaking organization determines how it views the leaking process, transparency, whistleblowing, and leaking itself. The model is not perfect, but leaking organizations can be roughly placed on a spectrum of ideologies from radical
transparency to selective release. The diagram below shows this spectrum with leaking organizations placed on it.

![Figure 1. Spectrum of Transparency Ideologies](image)

Radical transparency means releasing absolutely everything. A radically transparent leaking organization would have a website that listed all data on all visitors and a submission form that automatically posted the document and the information of the source with no modifications. The people who run the organization would post all information they came across in their lives. This is impossible but it represents one extreme of the spectrum.

Selective release means releasing the minimum information possible and all information being released with a specific agenda. Technically, the spectrum could end at no release of information but this is a spectrum of leaking organizations which inherently release information. A FOIA-resistant government agency that begrudgingly declassified only information that would aid the organization, serve as propaganda, or harm an adversary would be close to the selective release end. This end of the spectrum represents both increased secrecy and leaking as an extension of authority.

Both extremes on the spectrum of transparency ideologies are quite problematic. Indeed, the extremes are actually similar enough (Birchall, 2011) that the spectrum may be better portrayed as a loop. If a leaking organization released all information it possibly
could, there would be too much information available for any of it to be useful, and few people would want to interact with the leaking organization for fear of their personal information being released. Thus, the leaking organization would stop receiving information. Similarly, an organization that released almost no information would be unable to interact with the world and would eventually shut down.

As a result, most or all leaking organizations fall somewhere in the middle of the spectrum, but few can be placed exactly in the center of it. Organizations focused on transparency and promoting free information usually fall closer to the radical transparency end, while organizations whose priority is whistleblowing and correcting wrongdoings usually are closer to the selective release end. The exact placement on the spectrum also varies based on the goals and priorities of the leaking organization.

III. General Leaking Process

The ideological placement of a leaking organization on the transparency spectrum significantly changes the leaking process. For example, Cryptome, a leaking organization closer to the radical transparency end of the spectrum, tries to avoid making changes or adding any information to the documents because it contributes to the problem of leaking as an extension of authority (Cryptome Interview). On the other hand, Juzne vesti, an organization closer to the selective release end, uses leaked documents as a supplement to articles that contain background information and their interpretations of a situation (Juzne vesti Interview). Despite these differences, leaking organizations seem to share a general process. This broad leaking process derived from my case studies is outlined in the chart below.
This diagram looks at the process primarily from the perspective of the leaking organization. The source leaks documents and post-release actions are there to capture steps the source or others take before and after the release in which the leaking organization may be involved. These vary widely, not only based on the organization, but also the source and leaked information.

The organization receives documents step involves the organization getting the documents from the source in some form. The method of transmission can vary widely, as can the documents transmitted. Documents here refers to any leaked information from millions of emails to a tip about corruption. The level of involvement of the leaking
organization in this step also varies as some organizations advise sources on security practices and have secure submissions systems while others leave security to the source. Additionally, a few organizations find some of the documents they release (Public Intelligence Interview).

Leak processing is the intermediate step where leaking organizations prepare documents for release by making the information usable and safe. This is the primary focus of most leaking organizations and generally the most time consuming step (“Why WikiLeaks' bid for radical transparency failed”, 2012). There are three parts of this step and their exact order varies by organization and release: verification, redaction, and analysis/formatting. The verification sub-step involves tasks like checking the authenticity of a document and determining if the leak meets the organization's criteria for release. The redaction sub-step includes the removal of any information from names to metadata to parts of the document. The analysis/formatting step is any summary, addition of background information, mention of wrongdoings, or general preparation for release. The specific approach to these sub-steps depends on the organization.

The release step is the posting of documents, supplementary information, or articles from media partners. This could be followed by interviews about the release, advocacy for reform, or other post-release steps to help increase the effectiveness of the release.

Unfortunately, the leaking process lacks transparency. The post-release steps are usually publicly visible and the pre-release steps are often documented on the organization's website, but the leak processing step is shrouded in mystery. Some generalities can be implied by release practices of the organization, but specific details must be pieced together like a puzzle from interviews, assumptions, and rumors. This
should not be necessary and will lead to misunderstandings. This intermediary step is the primary function of leaking organizations, yet the most difficult (Roberts, 2011). Thus, it is important the organization improve the leak processing step as much as possible as it determines the effectiveness of a release and the leaking organization in general (“Why WikiLeaks’ bid for radical transparency failed”, 2012). While the exact definition of effectiveness will vary based on the organization's transparency ideology and approach, leak processing is universally important.

It is crucial that the leaking organizations be more transparent.LeaksWiki is an attempt to increase transparency in the leaking with the goal of making leaking organizations more effective by improving their process within the context of their transparency ideology.

IV. Case Studies

I used qualitative case studies to help answer my research question. A case study approach was necessary in part because a leaking organization’s methods cannot be separated from the goals of the organization. For example, a leaking organization with a philosophy of radical transparency will likely have a different approach to leaking than one that only seeks to correct wrongdoings. Similarly, the goals of a leaking organization cannot be removed from the context or role of the organization. An investigative journalism part of a mainstream news publication may have different goals than an independent leaking website run by a single person. The tools used may also be related to the methods, goals, and role of the organization. The effectiveness of the methods and tools used can only be measured within the context of the leaking website’s goals and
philosophy. This in-depth understanding of each leaking organization and if the general leaking process laid out above applies to it can only be gained through case studies.

Five case studies were done on a broad range of leaking organizations to allow for both comparisons between the sites and an understanding of potential variation. The five leaking organizations studied demonstrated a wide range of philosophies and goals from Cryptome’s near radical transparency to Associated Whistleblowing Press’s highly structured process to Juzne vesti’s sole focus on correcting wrongdoings. The case studies include leaking organizations roughly based in four different countries. The leaking organizations examined range from centralized and run by one person to distributed organizations with local nodes.

Interviews were the primary method for four of the case studies but these were supplemented with other information. Despite often being advocates of transparency, there is little public information about the internal processes of leaking organizations. Interviews were the best way to get this information. These interviews were made publicly available through LeaksWiki to help remedy the lack of information about leaking websites. The case study on WikiLeaks was conducted solely based on articles, papers, and interviews done by others.

The interviews were conducted via online chat or email. The exact questions varied by leaking website and method of interview. Questions that were not applicable were not asked and those with sufficient answers on the website were also not asked. The order of the questions and the follow-up questions asked depended on previous responses. Generally, the interviews tried to discern the goals and philosophy of the leaking website, the leaking process used, who was involved in the leaking process and how, the tools and methods used as part of the leaking process, and the effectiveness of
the leaking website in the context of its goals. The information gained from the interview was supplemented with details from the leaking website itself, qualitative observations of leaked documents and any information provided with them, outside articles and coverage of both the leaking website and its releases, and sometimes information on the leaking organization from books and papers. The case studies are framed in terms of the process outlined in the section above.

**Cryptome**

Cryptome is a leaking website that was created in June 1996. Cryptome is run by John Young and Deborah Natsios (Natsios and Young, 2012). It is one of the longest running leaking websites. They focus on documents related to "freedom of expression, privacy, cryptology, dual-use technologies, national security, intelligence, and secret governance" but accept and publish any documents (Cryptome).

*Transparency Ideology*

One of the primary goals of Cryptome is to decrease the power and influence of authority. "If a document will annoy, and best, deeply anger, believers in authority then it gets published" (Cryptome Interview). Another ideal outcome of Cryptome’s releases is “that many other persons will disclose sensitive and informative documents and other forms of publicly accessible, non-secret information" (Cryptome Interview). Furthermore, they believe that that “leakers and leak sites are authorities in sheep's clothing. The biggest and most prolific leakers are authorities leaking ...by any means to manipulate public understanding and behavior” (Cryptome Interview).
Cryptome does not seek to be primarily a leaking organization. While they do publish leaked documents, they “prefer libraries over leakage in which leaks may be implanted but are not the primary goal” (Cryptome Interview). The reason for this seems to be the aforementioned position that leaking websites are an extension of authority but also because leaks extend authority by virtue of being “a publicity gimmick”. For Cryptome, leaks are a tool to subvert authority by encouraging “self education”, “criticism”, and “thoughtfulness” (Cryptome Interview).

Cryptome publishes almost everything they receive with few changes. They focus on somehow restricted documents but will also publish openly available documents and relevant content from elsewhere. While they have not received any court orders to remove documents, Cryptome's home page notes than any court orders received or amusing bluffs will also be published (Cryptome).

People and Groups Involved

Cryptome is run by John Young and Deborah Natsios. They appear to be the only people involved in receiving, processing, and releasing documents. Cryptome receives documents from many different sources. Generally the source is not known but in some cases, like when John Young posted WikiLeaks-related emails he received or interviews he did, the source is known. While Cryptome does receive interview requests from media, they do not seek out media partners or others to help in the leaking process (Cryptome).

Cryptome does not use tools "beyond what any computer user has" to process documents (Cryptome Interview). The documents are released on http://cryptome.org/ in their raw form. Cryptome does not make any promises about the security of visitors or
sources and asks them to protect themselves. They do, however, list PGP keys on their website so it is possible to send Cryptome encrypted emails and documents. Cryptome also notes that they regularly delete logs.

**Leaking Process**

**Source Leaks Documents**

Cryptome explicitly tells sources it will not protect them. They also state that "Cryptome is not trustworthy, and lies", which fits in with their philosophy of leaking as an extension of authority. Cryptome does, however, provide a PGP key so sources can send encrypted documents and emails. Cryptome also does not collect user data and deletes logs but they still caution visitors to protect themselves (Cryptome).

While many documents are sent to Cryptome by outside sources, John Young also regularly publishes interviews done with him, posts from mailing lists (both closed and open lists), and other relevant material he finds directly in a list of offsite documents (Cryptome).

**Organization Receives Documents**

Cryptome receives documents via email, fax, or mail. Leaks are received by John Young. He may have to decrypt emailed documents if the source used encryption (Cryptome).

**Leak Processing**

Cryptome does very little leak processing because they believe context is "authoritarian nonsense" and "do not believe in verification, authentication, background,
foreground, advertising, promotion, branding, corporatization, any form that enlarges the
gap between individuals and those who claim to protect them, educate them, save them
from the devil, advocate national security racketeering, supports official, secret spying at
home and abroad” (Cryptome Interview). Despite this, even Cryptome generally does
something for each of the following steps and it performs them in the order listed.

**Verification**

Cryptome does not verify the authenticity of documents. While most documents
received are published, some are published with a delay and not all of John Young's
emails are put on Cryptome. Cryptome might not check the authenticity of documents but
it is clearly doing some filtering to determine what to publish. For some documents, like
the interview this case study is based upon, this filtering step could just mean waiting
until the document is complete (“Media.MIT Interviews Cryptome”, 2012). Additionally,
the Cryptome website says to start emails with "Cryptome." so some of the filtering could
be literal email filtering designed to separate documents intended for Cryptome from
other emails (Cryptome). Spam is also not posted.

**Redaction**

Cryptome sometimes removes names but not the names of people who "are
supporters of authority". For them, supporters of authority generally includes leakers and
leak sites. Cryptome did, however, remove most of the names in the emails published
from the WikiLeaks mailing list early on (“WikiLeaks Leak”, 2007).

**Analysis/Formatting**
Cryptome does not do any summary or analysis. They do format the releases to make them easier to read. Formatting is the most time consuming part of the process, but it is still quick (Cryptome Interview). Most of the formatting seems to be adding headlines, reformatting emails, adding captions under images, uploading material to the Cryptome servers, putting images directly on the web page, and pasting in links or quotes. The origin of the document is sometimes listed in a sentence at the top of the page (Cryptome).

**Release**

Documents are published on the Cryptome website with the most recent documents listed on the front pages and others available elsewhere on the website (Cryptome). Some documents are also tweeted by the Cryptome Twitter account, @Cryptomeorg (@Cryptomeorg Twitter).

**Post-Release Actions**

Cryptome does not actively organize publicity campaigns or do advocacy around their releases. John Young will occasionally do interviews about Cryptome in which he mentions some releases (McCullagh, 2010).

**Effectiveness and Outcome**

Cryptome has been quite effective at angering authority. John Young has been visited by the FBI on a few occasions (“FBI Visits Cryptome”). The FBI expressed concern that the information on Cryptome could be used to harm the United States but also stated nothing illegal was published. On a previous occasion, the FBI requested the
removal of a document and Cryptome refused but no court order was served ("FBI Requests PSIA Lists Removal", 2002). Cryptome has also received other takedown notices although they never received a court order, so no documents have been removed. Due to their tendency to anger authority, Cryptome has also had problems with their original ISP, Verio, refusing to continue hosting Cryptome ("Verio dumps controversial cryptome site"). They then moved to Network Solutions but were shut down there as well, potentially due to documents that list the names of malware being interpreted as malware ("Cryptome Shut by Network Solutions", 2012). Network Solutions later apologized, but Cryptome had already switched ISPs.

Additionally, PayPal froze Cryptome's account in March 2010 and although the funds were released, PayPal did not provide any details on why the account had been frozen (Serendipity, 2010). So insofar as their goal of angering authority of all sorts, Cryptome has been amazingly successful.

Cryptome has undoubtedly influenced other leaking organizations that came after it. As John Young seems to dislike many leaking organizations, this influence could be considered counterproductive. Still, these leaking organizations increase the flow of information and anger authority more, even though they themselves serve as an extension of authority. Thus, Cryptome's influence on leaking may be considered an effective, but not ideal, outcome. Leaking websites of a different form or libraries would fit better with Cryptome's goals (Cryptome Interview).

**Juzne vesti**

Juzne vesti is a Serbian investigative journalism organization started in August 2009 that receives leaked documents and information via an anonymous submission
system. Their releases seem to focus on five cities, Leskovac, Nis, Pirot, Prokuplje, and Vrange (Juzne vesti website).

**Transparency Ideology**

Juzne vesti uses articles based on leaked information to reveal and stop corruption in corporations and the government. Their other goals are to inform people about their rights and increase transparency generally. Juzne vesti only publishes verified information that reveals wrongdoings, and even then only the information needed to understand the specific wrongdoing discussed in the article. In their words, "if we have 100 pages of some contract, we will publish only the one that is directly related to article" (Juzne vesti interview). Juzne vesti supplements the leaked information with quotes, images, other documents, and videos they find that may help the readers fully understand the situation discussed in the article (Juzne vesti interview).

Juzne vesti operates as a media organization but receives information from both whistleblowers and leakers. They define a whistleblower "as person who believe in justice and is blowing in whistle to alarm on some wrongdoing, now expecting special reward for that" and distinguish whistleblowing from leaking which "can be motivated by some other goals (political, social, economical,..." (Juzne vesti interview). Regardless of the goals of the source, Juzne vesti publishes information if and only if, it meets their release criteria outlined above (Juzne vesti interview).

**People and Groups Involved**

Juzne vesti is a media organization that, as of December 2012, consists of twelve journalists primarily working on Juzne vesti. All of the journalists working on Juzne vesti
are under the age of thirty-five and the average age is twenty-seven. They also have additional journalists with whom they collaborate (Juzne vesti interview).

The source of a leak can be anyone but they sometimes receive leaked information from public officials who disagree with their party on an issue. If they agree with the stance of the official, they publish the comment anonymously but maintain records of their communication. Juzne vesti also sometimes receives information from people trying to discredit public figures like their political opponents and ex-girlfriends (Juzne vesti interview).

Juzne vesti has consultants with whom they discuss the leaked information, ask for additional information, or verify the documents they have. Their pool of consultants includes the "former Supreme state auditor, former prime minister, former mayors" (Juzne vesti interview). Other officials who may know of the existence of a document revealing corruption may also be called to comment (Juzne vesti interview).

Leaking Process

Source Leaks Documents

Sources submit documents through the free and open source GlobaLeaks submission system accessible at perun.juznevesti.com. They suggest but do not require that sources use Tor for anonymity. Additionally, the submission system website tells sources if Tor is properly configured or not. Their submission form allows sources to type information and upload documents. Sources can also check on the status of their submission (Perun, Juzne vesti).

As noted above, Juzne vesti sometimes receives documents or information from public officials although anyone can submit documents. Most of the information they
receive relates to government and sometimes corporate corruption, often at the local level (Juzne vesti interview).

Organization Receives Documents

The journalists at Juzne vesti normally receive the documents. If the source wants to remain anonymous, and they know the identity of the source, they will discuss this when they receive the documents (or perhaps even before they are sent). Juzne vesti normally gets leaked information through its submission system, but it might receive additional information through FOIA requests or their pool of contacts (Juzne vesti interview).

Leak Processing

Based on the interview, it sounds like Juzne vesti typically first verifies the leaked information, then does additional research (sometimes as part of verification) and writes the article, and finally adds only the relevant and redacted leaked information to the article (Juzne vesti interview).

Verification

Juzne vesti verifies all information it releases. They say "everything we receive we see only as a clue, nothing more" (Juzne vesti interview). Ideally, their releases and documents are verified via the Freedom of Information Act (FOIA) but they may not always receive a response and sometimes the issue is time-sensitive so a FOIA request would take too long. In this case, they call public officials related to the situation and ask them to comment. This can even be used to verify the existence of documents they may
not have in their possession (which can be enough for an article). One example from the interview is as follows.

"for the story about heating plant (director hired her son), I have received information in Friday, few hours after she had signed the contract and guy should start to work from Monday. I did not have a time to send FOIA (they have 15 day to answer, but if they dont I have to appeal to Commisioner and whole process last at least 2-3 months), so I have called director and I said to her that I have those contracts (I was lying, I only had information about them), and asked her for comment and she can confirm me the authenticity. She said that she dont want to comment but have offered me to come to her office during next week and she will show me contracts - that was enough for me - indirectly she had confirmed that contracts exits" (Juzne vesti interview)

The verification step also includes verifying that leaked information meets publication criteria. For Juzne vesti, this means identifying evidence of corruption (Juzne vesti interview). This could happen either before or after they verify the authenticity of a document.

Redaction

The most notable form of redaction is that Juzne vesti removes all parts of the document not relevant to the wrongdoing at hand from the release. Juzne vesti does not remove the names of public officials, but they do remove information like an official's date of birth or address. This information is blacked out when the document is published. They also sometimes publish anonymous comments from public officials or other related sources under specific conditions outlined in the People and Groups Involved section above (Juzne vesti interview).
Juzne vesti does not directly remove document metadata that could be used to identify the source, but they use the GlobaLeaks submission platform which will support metadata removal in the future (Pietrosanti, 2012).

**Analysis/Formatting**

Juzne vesti is primarily an investigative journalism outlet, so all leaked information is released in article form. For these articles, they collect statements from everyone mentioned in the article if possible. Juzne vesti also has a group of public officials who they may call for comment or additional information. The redacted leaked information relevant to the article is released as a part of or in addition to the story. They also add any relevant background information or summary of unreleased parts of a leaked document (Juzne vesti interview). Juzne vesti may also modify the documents they release to draw attention to the part that reveals corruption (Gasoline spending document, 2012).

**Release**

Articles based on leaked information are posted on the Juzne vesti website, specifically in a section focused on investigative journalism. Relevant leaked documents and other supplementary information are posted with the story (Juzne vesti website).

**Post-Release Actions**

If a wrongdoing is corrected after Juzne vesti writes a story about it, they may add a note to the original article or write a follow-up story describing how the issue was handled (Skidaju sporne znake, 2012).
**Effectiveness and Outcome**

Juzne vesti has been very effective within the context of their goals. On numerous occasions, their stories have caused public officials to quickly correct the wrongdoing. In the interview, they gave a few examples of times this occurred.

- "We have published the story that the brother of mayors chief of stuff started working and immediately become chief in one city owned company, but there was no any public contest for that position. It is important to mention that new mayor was elected in mid July, and one of his key argument was "there will be no political employments in public sector". Day after we have published article, mayor released statement that his chief of stuff brother was fired (Partijsko-porodično zapošljavanje u Nišu, 2012).

- After Juzne vesti released article that city owned building directorate have just published contest for pawing 5 streets that were already been pawed (unofficially, they have hired one building company to pawe streets, but without contest. So, they had to publish contest later to try to cover everything), Directorate have canceled the contest (Hteli da asfaltiraju već asfaltirane ulice, 2012).

- We have published article the general manager of city owned heating plant (the only one in city) had hired her son and daughter of her assitant, and give them chief positions. 7 days later she was fired (Direktori Toplane zaposlili svoju decu, 2012).

- Only few hours after we have published article about some road sign that was placed on sidewalk in the middle of track for blind, that sign was moved" (Skidaju sporne znake, 2012). (Juzne vesti Interview)

It is also worth noting that Juzne vesti has gained quite a bit of publicity both as one of the few investigative journalism organizations in Serbia (USAID Serbia, 2012) and due to their use of an anonymous submission system enabled by tools like Tor and GlobaLeaks (Murrock, 2012). They have also received several awards for their journalism (IREX Serbia, 2012). Investigative journalism is not widespread in Serbia so Juzne vesti is a pioneer in media-driven transparency (Juzne vesti interview).
Public Intelligence

Public Intelligence is an anti-secrecy organization created in summer 2009 that publishes sensitive or restricted information. Most of their information is obtained from public sources (Public Intelligence website).

Transparency Ideology

Public Intelligence believes "access to information is a fundamental human right, allowing individuals and societies to orient themselves, make decisions and have some modicum of control over their own lives" (Public Intelligence interview). The goal of Public Intelligence is to make available as much restricted information as possible to a wide audience in an accessible format so people can use and benefit from the information. They also avoid attempts at censorship in order to keep this information online (Public Intelligence interview). They publish documents they deem to be in the public interest and avoid adding external information. Public Intelligence uses only facts and excerpts from the documents they publish to make the information more accessible while avoiding bias. All documents are published completely and unedited, aside from minimal redactions (Public Intelligence interview).

They dislike both the terms leaking and whistleblowing. "Leaking sounds like an accident and is a favorite tactic of those in government. Whistleblowing sounds like something done by a hall monitor in grade school. Telling the truth shouldn't require special terminology. We should endeavor to build a culture that is built upon truth-telling and openness, rather than one that lauds these activities as praiseworthy or unusual in nature. Public Intelligence publishes information that is of value and then tries to defend that information from attempts to censor it" (Public Intelligence interview). Instead,
Public Intelligence seems to think of their organization as an anti-secrecy organization (Kent, 2010) or a "collaborative research project... defending the public's right to information" (Public Intelligence website).

**People and Groups Involved**

Public Intelligence states that "not many" people are involved in preparing documents for release (Public Intelligence interview). Those who are involved are "independent researchers around the globe." (Public Intelligence website). While Public Intelligence has a submission system on their website, many of their documents are obtained by people involved in Public Intelligence or people they know. In the past, Public Intelligence has used public forums to crowd source its leak analysis process but stopped due to a lack of meaningful contributions. Public Intelligence does not provide documents to reporters before release. They have, however, discussed documents with reporters prior to release (Public Intelligence interview).

**Leaking Process**

**Source Leaks Document**

Public Intelligence accepts submissions via an encrypted contact form on their website or email. A PGP key is provided for the purpose of encrypted emails (Public Intelligence website). In practice, they obtain many of the documents they publish themselves. According to the Public Intelligence interview, obtaining documents is the most time consuming part of the leaking process because "people are rarely, if ever, going to risk their lives and/or livelihoods to come and drop material in your lap. This is one of the things most people don't understand about so-called "leak" sites: they receive far
fewer "leaks" than you would imagine" (Public Intelligence interview). The documents themselves originate in many different governments and organizations, private and public, around the world (Public Intelligence interview).

**Organization Receives Document**

Public Intelligence receives information via their encrypted contact form integrated with wordpresss and email if they did not obtain the document directly. The people who run Public Intelligence are the ones who receive the document or information and prepare it for release. There are no media partners or others who receive the document before release (Public Intelligence interview).

**Leak Processing**

Public Intelligence first determines the value of a document and then analyzes/summarizes it before release. In some cases, some parts of a document are redacted. All software used throughout the leaking process is free and open source (Public Intelligence interview).

**Verification**

Upon receipt of a document, Public Intelligence determines if it is worth further verifying, analyzing, and releasing. Some of the questions used to determine the worth of the document include "Does the document describe or reveal something about a public process? Does the document relate information that is informative or educational in a broader societal context? Who produced the document and what are the rules/laws governing its disclosure or publication? Has someone else already published the
document? Does the publication of the document contribute in some way to the body of available information on a topic of public importance?” (Public Intelligence interview). If the document is valuable enough, Public Intelligence continues the analysis.

Public Intelligence generally has little need to verify the authenticity of documents because they say “we often know the source of a document directly because we obtain the documents ourselves and can thus determine their authenticity, provenance and purpose by understanding the nature of the source from which we obtained them” (Public Intelligence interview).

**Redaction**

Whenever possible, Public Intelligence avoids redacting documents because that "would defeat the purpose of making information freely available" (Public Intelligence interview). They do sometimes remove personal information like social security numbers or information that could lead to the discovery of the source of the documents. Public Intelligence rationalizes the latter within their transparency ideology by saying that "over time, this allows for more information to enter into the public domain than if we were to simply post the document with nothing removed" (Public Intelligence Interview).

**Analysis/Formatting**

While Public Intelligence believes that people must "create context, meaning and relevance for the information themselves," they do try to make the information they release more accessible. They do this by providing quotes, lists of facts, and summaries along with the leaked document. In these, Public Intelligence tries to "explain the
material in a manner that attempts to limit our own personal biases” (Public Intelligence interview).

This step is probably the most difficult part of Public Intelligence's leaking process as they "struggle often with how to make complex material accessible and relevant to audiences that are not necessarily motivated to understand it" (Public Intelligence interview). In one case, they tried to crowd source the analysis process for a set of documents about the war in Afghanistan using a forum, but few people provided meaningful information (Public intelligence interview).

Summaries/analyses also seem to be formatted for readability before release, but documents are provided in their full and unedited original form (Public Intelligence website).

Release

Documents are published on the Public Intelligence website (which uses Wordpress) along with the summary/analysis based directly on the document. Documents are not directly released on any other websites or by other organizations (Public Intelligence interview).

Post-Release Actions

Media organizations do publish articles about Public Intelligence releases (Franceschi-Bicchierai, 2012) (Franzen, 2012). Public Intelligence does discuss releases their implications with reporters writing about them (Public Intelligence interview).

Effectiveness and Outcome
Public Intelligence has been very successful in publishing a lot of valuable information. They make daily releases with understandable and useful analyses. Hundreds of their releases have also been covered by media of some sort and many more have been cited by other sources. Unfortunately, the most widely covered releases are popular "due to some salacious or attention-grabbing quality, not necessarily their true informational value". An example of one such release is given by Public Intelligence, "we published a document and an article earlier this year on an IARPA program called Catalyst that is designed to act as an "entity extraction" and "semantic integration" system across the entire intelligence community. The system is designed to parse large-scale datasets and automatically extract and organize meaningful information for storage and analysis in later investigations or intelligence gathering. It's a dry topic, but has tremendous implications for a number of issues like widespread electronic surveillance. Basically no one paid any attention to this. On the other hand, a few months prior we got a story into the mainstream media that was so popular that it was reported everywhere from Indian TV to Good Morning America. It was about how apparent gibberish in [an] early version of an al-Qaeda magazine was in fact cupcake recipes. There were headlines like "Al-Qaeda Mag Attacked in Operation Cupcake."" (Public Intelligence Interview) (Gardham, 2011). Their website does mention, however, that part of their purpose is to highlight information that might be ignored by the mainstream media in articles like the one described above.

While their analyses are good, Public Intelligence notes that they struggle with both making the information accessible and meeting their standards of objectivity in their summaries. They also have difficulty getting people to pay attention to many of the documents they publish that are not attention-grabbing (Public Intelligence interview).
Public Intelligence has been extremely successful at keeping documents online. They have a whole section of their website dedicated to the many different threats and takedown notices they have received from a variety of different organizations, but no document has ever been removed (Public Intelligence interview).

Associated Whistleblowing Press

The Associated Whistleblowing Press (AWP) is a media agency founded in September 2012 that releases leaked information. AWP maintains its central node and newsroom (whistle.is) and also works with local nodes like Ljost. They are experimenting with new leaking tools through projects like their crowd sourced analysis of WikiLeaks's Cablegate releases, cablegate.awp.is. Additionally, AWP runs a wiki, leaks.cc, to coordinate analysis of leaked information and documents.

Transparency Ideology

The Associated Whistleblowing Press focuses on releasing only restricted documents that either reveal a wrongdoing or are significant in their own right. All documents that meet these standards are released. AWP releases documents relevant on the local level with the hopes that the information will have a greater effect on local issues. While AWP would like to correct or highlight wrongdoings with their releases, their overall goal is to contribute to "an improved public control of institutions, accountability for their actions and so on" (AWP interview).

AWP defines leaking as "the activity to make secret information be publicly accessible" and describes whistleblowing as "an ethical leak" (AWP interview). They also suggest that leaking and whistleblowing have been converging as transparency and
free information movements aim "to propagate and make public restricted information which is of public interest" (Noel, 2012). While AWP considers itself an organization focused on whistleblowing, they also hope to encourage a culture of transparency so more information of public interest is made available and corruption revealed (AWP interview).

**People and Groups Involved**

The Associated Whistleblowing Press is unique in that they work with many local nodes to process documents. In certain cases, they may also work with outside experts for tasks such as checking for forgery of documents. Articles about leaked information or documents are also written by media partners and published on whistle.is, their centralized newsroom. AWP is experimenting with crowd sourcing platforms for document analysis so more people may be involved in the future (AWP interview).

**Leaking Process**

**Source Leaks Documents**

The Associated Whistleblowing Press uses the GlobaLeaks framework for document submission. Each local node has a submission system on its website. Different levels of caution are outlined on a page that provides instruction to the source on how to safely submit documents. The standard method asks the source to use the Tor Browser to access their submission system. The safer and safest methods suggest sources encrypt files they are submitting with GPG and/or the TAILS operating system and to send documents only stored on a flash drive from a public Internet hotspot. They also suggest
not telling anyone about the submission (Ljost Submission Page). All of the tools they suggest sources use are free and open source.

Organization Receives Documents

While local Associated Whistleblowing Press nodes have submission systems on their websites, all information goes directly from submission to the central AWP servers in Iceland. AWP then shares the information with the relevant local node(s) for analysis (AWP interview). All information is stored offline until the analysis and leak processing is complete (AWP website).

Leak Processing

Generally, AWP verifies a document first, and then does redaction during the analysis step. Some parts of the verification or analysis steps could take place after release.

Verification

The Associated Whistleblowing Press first reviews the leaked information to verify that it meets their publication standards. That is, the leaked document must "prove corruption and abuse" and not be a firsthand account or rumor (AWP interview). More broadly, AWP also accepts any "restricted or censored material of political, scientific, ethical, diplomatic or historical significance" (AWP website).

After checking that a leak meets their publication criteria, AWP has two pre-release steps in their verification of document authenticity process: conceptual and electronic cross-checking. Out of these two steps, conceptual cross-checking is generally
more important. Conceptual cross-checking is conducted mostly by the local nodes who read a document and check for accuracy in "historical facts, actors and their behaviours." For electronic cross-checking, AWP works with forgery experts who use unspecified tools and techniques to verify the authenticity of photos, videos, and scanned documents. Automated tools for electronic cross-checking are still in progress (AWP interview). The motives, cost, and difficulty of forgery are also considered throughout the process (AWP).

After release, the organization the document or information comes from can verify its accuracy. This can be done both directly, through a request that the information be taken down, and indirectly, when an organization says some of their classified or restricted documents were released. If information is verified post-release through one of these methods, AWP notes this on the document release page. While not all documents are verified externally, all pass the internal conceptual and electronic cross checking tests (AWP interview).

**Redaction**

The Associated Whistleblowing Press engages in two types of redaction: removal of metadata and removal of names. AWP removes metadata in documents because some metadata can indicate who the source is or provide information that would make the source's identity easier to determine (AWP website). They do not disclose the methods and tools they use to remove metadata as it would make documents easier to forge but AWP did say that most of the metadata cleaning was done manually. AWP removes names of any third parties not involved in the wrongdoing at hand. They do not note any
other cases where information is removed from the documents they publish (AWP interview).

**Analysis/Formatting**

The Associated Whistleblowing Press has two steps in their document analysis process, an initial classification and tracking read-through and the writing of news articles that analyze the documents to put them in context. The classification and tracking read-through step is mostly important for long documents or sets of documents. Documents are read through and relevant information is noted and tracked. They are still working on a system for tracking documents. Ideally, this system "should cover all the types of fields, be searchable through these fields, have commenting features and selection of different 'status modes' for each single file" and it should also have "the ability to cluster files into pre-determined rules (by tags, keywords, field types, size, type of file etc)" (AWP interview).

In the second part of the analysis step, journalists write articles about the documents. These articles put the documents into their broader context by "explaining actors, motives and consequences in relation to the organizations or states in question" (AWP website).

AWP is currently experimenting with a crowd sourcing platform, cablegate.awp.is, where people can write notes and stories about WikiLeaks cables. They also have a graph tool that shows shared references and links between cables to aid in the analysis process. If their trial with WikiLeaks Cablegate documents goes well, this could be an alternative or supplement to the second step of the AWP analysis process in the future (AWP interview)(cablegat.awp.is).
Release

The Associated Whistleblowing Press releases all the documents from the local nodes and the articles about them from the analysis step on the AWP newswire, whistle.is (whistle.is). These or other articles may also be published elsewhere by media partners, perhaps in the local media (AWP interview).

Post-Release Actions

Local AWP nodes may engage in advocacy efforts or additional publicity in both traditional and non-traditional media after leaked information is released. Although the exact method is not yet clear, AWP hopes to incite "a collective response to any issues" (AWP interview).

Effectiveness and Outcome

It too early to judge the effectiveness of AWP because it is very new, only has one running node, and has not published any documents of its own yet (AWP interview). Despite this, AWP has published articles based on documents leaked by other organizations (whistle.is). Additionally, a few days after release their collective Cablegate analysis tool has almost 200 cables tagged (cablegate.awp.is). So far their platforms, processes, and tools seem to be working well with these tests.

WikiLeaks

WikiLeaks is a leaking organization founded in 2006 that publishes restricted documents and information (WikiLeaks website).

Transparency Ideology
WikiLeaks engages in what it refers to as "principled leaking" (WikiLeaks website). According to their website, "WikiLeaks interest is the revelation of the truth. Unlike the covert activities of state intelligence agencies, as a media publisher WikiLeaks relies upon the power of overt fact to enable and empower citizens to bring feared and corrupt governments and corporations to justice". While WikiLeaks tries to publish most or all of the material they receive, they have limited time so they "look for and prioritize acts of injustice that expose abuse within the material" (Assange WikiSecrets interview, 2011). WikiLeaks does not publish "rumor, opinion, other kinds of first hand accounts or material that is publicly available elsewhere" (WikiLeaks wiki). Overall, WikiLeaks seems to promote transparency as a political tool to help people reduce corruption.

Julian Assange stated in an interview that "the government doesn't have a right to secrets" but also notes that sometimes it may be appropriate to temporarily withhold information (Assange WikiSecrets interview, 2011). WikiLeaks does recognize the right to the privacy and security of sources and innocent people (WikiLeaks wiki). WikiLeaks seems to follow policies based on these statements in their releases as documents are regularly held back to finish redaction and review. In some cases, they wait to release documents until a situation changes or stabilizes (x7o, 2010).

People and Groups Involved

Aside from the sources, there seem to be three categories of people involved in WikiLeaks, staff, volunteers, and media partners. The staff seems to be a small group of people shifting in number who are paid to work on WikiLeaks or use their own money to help with WikiLeaks full time. In January 2010, the staff was five people (Assange interview with Mey, 2010). The most visible person in this category is the WikiLeaks
spokesperson, Julian Assange. Kristinn Hrafnsson is also described as staff on the WikiLeaks website (WikiLeaks website). Volunteers are those who are not paid and help part time with WikiLeaks. Some volunteers help directly with the releases or the operation of WikiLeaks. Active supporters who help WikiLeaks through websites like WL Central or lawyers who help WikiLeaks pro bono could also be considered in the volunteer category. Finally, WikiLeaks has a pool of media partners who often help prepare releases or do background research (WikiLeaks website).

WikiLeaks also has an advisory board, but it is not clear if they do anything (Rintoul, 2010). The circumstances of WikiLeaks's founding are similarly vague because many of the founders do not want to be identified (“Why are the WikiLeaks Founders Anonymous?”, 2010). It is known that Julian Assange was involved early on and that John Young of Cryptome originally registered the domain name (“WikiLeaks Leak”, 2007).

Leaking Process

The WikiLeaks leaking process has changed over time. There seems to be three models it has used: a collaborative wiki where anyone can post documents, controlled release with all resources focused on one or two releases, and collaboration with mainstream media partners to release material (Chen, 2011). All of these models are discussed to some extent but the most attention is devoted to the third and current leak processing model of WikiLeaks.

Source Leaks Documents
WikiLeaks prefers online submissions and asks sources to "upload the document and specify the language, country and industry of origin, likely audience, reasons for leaking and approaches to verification" during the leak (WikiLeaks wiki). WikiLeaks has previously provided anonymous drop boxes but there does not appear to be one currently available. For security reasons, they do not provide information on their drop box system. WikiLeaks does help sources find a way to submit material anonymously and securely. They also offer to provide sources with cover domain names for submission if they email them (WikiLeaks website). WikiLeaks also accepts submissions via mail at a post office box in Australia (WikiLeaks wiki submit page).

**Organization Receives Documents**

If the documents were submitted via the secure drop box when it still existed, after receipt "documents go into queue to obscure the date and time of their acquisition" (WikiLeaks wiki). The documents are also backed up on other WikiLeaks servers around the world. Staff, media partners, and perhaps some volunteers receive the material for review (WikiLeaks wiki). If the material is sent via mail, it is handled by the "facilitator" at the address to which it is sent (WikiLeaks wiki submit page).

There are conflicting reports on how WikiLeaks obtained their original documents. Some sources say that the original WikiLeaks documents were intercepted from a Tor exit node (Zetter, 2010) but Assange denies this claim (Assange WikiSecrets interview, 2011).

**Leak Processing**

**Verification**
The first part of WikiLeaks's verification step involves WikiLeaks editors reading through documents to be sure they meet the release criteria. That is, the documents must be secret or restricted, significant, and not rumor or opinion or a first-hand account (WikiLeaks wiki).

The second part of the verification step is to check the authenticity of the documents. Before release, "WikiLeaks staff examine all documents and label any suspicions of inauthenticity based on a forensic analysis of the document, means, motive and opportunity, cost of forgery, what the authoring organization claims and so on" (WikiLeaks wiki). They also engage in verification by posting the leaked document for anyone to scrutinize, especially the "community of interest around the document" (WikiLeaks website). Sometimes they also collect external evidence to verify their biggest releases. This was the case with collateral murder where WikiLeaks sent journalists to Iraq to collect related statements and supporting documents (WikiLeaks website). Takedown notices and requests for the return of documents could also help verify their authenticity (Gearn, 2010). Finally, as stated above, WikiLeaks sometimes asks its sources to provide suggestions on how to verify the documents.

Redaction

WikiLeaks has a "harm-minimization" process where they remove information that could be used to trace the source like metadata and the names of innocent people from their documents (WikiLeaks wiki). There has been some concern that some releases are hastily redacted and names are missed (Hopkins, 2010). Some of the redactions appear to be automated as well, but WikiLeaks provides no information on any
automated redaction methods (Hopkins, 2010). In one instance, WikiLeaks accidentally released unredacted cables (Cheng, 2011).

**Analysis/Formatting**

Analysis/Formatting is one of the steps where the different WikiLeaks leak processing models diverge significantly. In the first model where they used a wiki, documents were posted on a wiki and anyone could edit the accompanying information (Chen, 2011). Accompanying these releases are summaries, background information, the source's notes about the document, information on the file, the date posted, verification status of the document, and additional sources (“The looting of Kenya under President Moi”, 2007). On some documents, some of these supplemental components seem to be missing (“Scientology Chain of Command”, 2008). When WikiLeaks was using a wiki, most of the formatting done was to adapt the information provided with the document to the wiki format.

The second model of analysis and formatting is demonstrated with the release of the video Collateral Murder. WikiLeaks edited Collateral Murder heavily to make the events in the video easier to understand. They then provided a whole website of supplementary information, explanations, and documents (Collateral Murder website).

The third model of analysis and formatting involves WikiLeaks's media partners writing articles to supplement, frame, and discuss the implications of the documents released (WikiLeaks submit page). With big releases, WikiLeaks will often coordinate media partner analysis and setup websites where viewers can browse the raw documents in an easy-to-read format. For email database releases, this might include neatly formatting all emails with a given subject in a table (GI Files website). WikiLeaks also
provides a system to search documents and manage releases (“WikiLeaks providing a trap for journalists, NGOs”, 2012).

In some cases, WikiLeaks has crowd sourced the analysis of their releases through the #wlfind hashtag and other crowd sourcing platforms made by supporters (@wlfind Twitter). While WikiLeaks has released analyses and summaries with some of their documents, some critics find that their efforts fall short and result in the release of useless information (Lovink and Riemens, 2010).

Release

When WikiLeaks used a wiki, the releases were all made on the wiki (Chen, 2011). Under their second release model, WikiLeaks released Collateral Murder at a press conference and on their website (Chen, 2011). Currently, WikiLeaks media partners post articles about documents, and WikiLeaks releases them at the same time in their raw form on their website or the website for the document set (“WikiLeaks setting another trap for journalists, NGOs”, 2012).

Post-Release Actions

Before and after release, WikiLeaks will publicize releases on their Twitter account. In the past, they have also tried to crowd source analysis of released documents through this account (@WikiLeaks Twitter). For big releases, WikiLeaks often holds a press conference before and/or after release (Afghan War Logs Press Conference).

Effectiveness and Outcome
While some people have questioned some of their release practices, and some of their releases have gone unread, WikiLeaks has been quite successful at achieving their goals. Their releases have been credited with inspiring the Icelandic Modern Media Initiative (Vallance, 2010), revealed unreported attacks in Iraq, provided detailed information on Guantanamo Bay (Leigh, 2011), and more. As of 2011, officials from the Pentagon said that WikiLeaks releases had not caused anyone to die (Youssef, 2011). This may have changed since.

V. Leaking Process

This section is a step-by-step discussion of the similarities and differences between the leaking organizations and how these different approaches still fit within the general leaking process model I presented.

Source Leaks Documents

All of the leaking organizations examined provide some way for sources to send encrypted documents. Cryptome and Public Intelligence post GPG keys so sources can send them encrypted emails and files (Cryptome interview)(Public Intelligence interview). Juzne vesti and Associated Whistleblowing Press use the free and open source GlobaLeaks submission system and have instructions on how to securely submit documents (Juzne vesti interview)(AWP interview). WikiLeaks did use a secure drop box similar to the GlobaLeaks system but that is not online now. They offer to help potential sources submit documents securely (Wikileaks website).

It is also worth noting that Public Intelligence obtains many of their documents themselves because "people are rarely, if ever, going to risk their lives and/or livelihoods
to come and drop material in your lap. This is one of the things most people don't understand about so-called "leak" sites: they receive far fewer "leaks" than you would imagine" (Public Intelligence interview). This seems to be true for the other organizations studied to some extent. WikiLeaks may have gotten their first documents from a Tor exit node (Zetter, 2010). Associated Whistleblowing Press has mostly analyzed WikiLeaks's Cablegate documents (AWP interview). Juzni vesti gets many of their own documents through FOIA (Juzne vesti interview). Cryptome has a whole section on their website for external documents, and many of the documents posted are emails John Young has received personally (Cryptome interview).

Organization Receives Documents

Cryptome and Public Intelligence receive documents directly via email (Cryptome website)(Public Intelligence interview). Cryptome also accepts documents via fax or mail. In both Cryptome and Public Intelligence, only the people running the organization see the document before release (Cryptome interview)(Public Intelligence interview).

AWP and Juzne vesti receive documents via their submission system or email (AWP interview)(Juzne vesti interview). AWP accepts submissions on the website of their local nodes but all documents go directly to their server in Iceland where they are stored offline. They are then retransmitted to the local nodes after an initial review (AWP interview). WikiLeaks has a similar procedure except it is media partners and not local nodes that may see documents before release (WikiLeaks about).

Leak Processing
These steps are done in a different order for each leaking organization. Notably, redaction is often done at the same time as analysis/formatting (AWP interview)(Cryptome interview). Verification is consistently done first unless a document is authenticated after release (AWP interview).

**Verification**

There are generally two parts to verification, checking if the document meets publication policies and verifying the authenticity of the document. The first step is done almost universally. Even organizations like Cryptome that publish almost everything they receive will wait until a document is complete before publishing it (“Media.MIT Interviews Cryptome”, 2012) and avoid publishing spam. Most of the organizations other than Cryptome have a more rigorous approach to this part of the verification step and make some judgment about the value of the information. In the case of Juzne vesti, the document must reveal a wrongdoing for them to proceed (Juzne vesti interview). For WikiLeaks and the Associated Whistleblowing Press, the leak needs to be significant or reveal a wrongdoing for it to be published (AWP interview)(WikiLeaks submit page). Public Intelligence tries to assess the public worth of a document. To do so, they ask the following questions: "Does the document describe or reveal something about a public process? Does the document relate information that is informative or educational in a broader societal context? Who produced the document and what are the rules/laws governing its disclosure or publication? Has someone else already published the document? Does the publication of the document contribute in some way to the body of available information on a topic of public importance?" (Public Intelligence interview).
These questions also seem to be similar some of those WikiLeaks or Juzne vesti may ask based on their publication policy.

After deciding if a document is worth their time, leaking organizations sometimes verify the authenticity of the document. Cryptome will very rarely verify the authenticity of a document, but it has on at least one occasion (“WikiLeaks insiders messages”, 2010) Generally, Cryptome states that they "do not believe in verification, authentication" (Cryptome interview). Public Intelligence normally has no need to verify a document because they say "we often know the source of a document directly because we obtain the documents ourselves and can thus determine their authenticity, provenance and purpose by understanding the nature of the source from which we obtained them" (Public Intelligence interview). While WikiLeaks cannot verify the authenticity of their documents by virtue of knowing their source, they do ask the source for suggestions on how they could best verify the document (WikiLeaks submit page).

Aside from verifying the authenticity of the leaked information based on the source, there seem to be a combination of four approaches used by WikiLeaks, Associated Whistleblowing Press, and Juzne vesti. First, the staff of a leaking website could file a FOIA request for a document or otherwise request the document directly from the organization that created it. In many cases, this is unlikely to work but provides high certainty of the validity of the document if it does work (although the organization involved could have created a fake document in the first place). Juzne vesti favors this tactic where possible (Juzne vesti interview). WikiLeaks supporters have used FOIA as an advocacy tactic as well (ACLU, 2011).

Second, the document could be verified indirectly by the organization that created it. This can result from the first approach when the document is not released, but its
existence is verified. Leaking organizations can also call people from these organizations and ask them for comments on the document. If they comment, the existence of the document is verified. This method is particularly useful if a leaking website has information about the document but not access to the document itself. While not as accurate or precise as the first two methods, the indirect verification method can be attempted in most cases. Juzne vesti has successfully used this method to ascertain the existence of documents they did not have (Juzne vesti interview). Associated Whistleblowing Press mentions this as a good method of verification as well (AWP interview).

The remaining two methods of verification rely less on response from or access to the organizations involved. Third, the leaking organization can cross-check the document for evidence of forgery based on the content. This could include searching for inconsistencies or inaccuracies in the historical or political facts mentioned. Conceptual cross-checking may also include analysis of motives for and the difficulty of forgery. A fake document can certainly get past conceptual cross-checking, but it has to be a very good fake. The conceptual cross-checking validation method also requires people who are very knowledgeable about the topics relevant to the leak. Fourth, the leaking organization can look for electronic evidence for forgery. Electronic cross-checking can eliminate obvious fakes but Associated Whistleblowing Press noted that electronic forgeries can be "almost perfect" (AWP interview). The exact methods used in electronic cross-checking were not specified. Both Associated Whistleblowing Press and WikiLeaks discuss these methods but provide few details on how they are performed. They do both mention that people who the documents are relevant to are likely to be the best conceptual cross-checkers (AWP interview)(WikiLeaks website).
Redaction

While only some organizations verify the authenticity of their releases, some level of redaction is near universal. Even the leaking organizations that tend the most towards radical transparency, like Cryptome, generally still remove some names for protection of sources and others (Cryptome interview). Public Intelligence, a leaking organization with a transparency ideology close to radical transparency, justifies their redaction policy by saying "over time, this allows for more information to enter into the public domain than if we were to simply post the document with nothing removed" (Public Intelligence interview). That said, most leaking organizations redact as little as possible (AWP interview)(Public Intelligence interview). The one exception to this is Juzne vesti. Juzne vesti redacts everything but the part relevant to the article they write (Juzne vesti interview).

Removal of names seems to be done by hand. There is some speculation that WikiLeaks sometimes uses automated redaction but that is not confirmed (Hopkins, 2010). Automated redaction may be necessary to manage large leaks.

In addition to removing names and identifying information, WikiLeaks and the Associated Whistleblowing Press also remove document metadata that could lead to the identification of the source (AWP interview)(WikiLeaks website). For this, they use a few unspecified tools, but AWP notes that they remove a lot of metadata by hand. The GlobaLeaks whistleblowing framework is currently working on integrating automatic metadata removal into their submission system so Juzne vesti and AWP will have the option for automatic metadata removal in the future (Pietrosanti, 2012).
**Analysis/Formatting**

Analysis/Formatting is the area where leaking organizations diverge the most based on transparency ideology. Cryptome only does basic formatting to make their releases more readable (Cryptome interview). Public Intelligence writes some summaries to go along with their documents, making them more accessible to readers. Otherwise, they try to avoid adding context or additional information, because any additional details would add bias to the supplementary information (Public Intelligence interview). Both Public Intelligence and Cryptome prefer to let the readers judge the documents themselves. Neither organization uses any special tools in their formatting and analysis process (Public Intelligence interview)(Cryptome interview).

WikiLeaks, Associated Whistleblowing Press, and Juzne vesti are different. Not only do these organizations add information to their releases, but they release the documents with articles placing them into a narrative and explaining their context. This is a stark contrast to Cryptome which states "We do not believe in "context." That is authoritarian nonsense" (Cryptome interview). For AWP, WikiLeaks, and Juzne vesti, analysis involves journalists reviewing documents and writing articles about them (AWP interview)(Juzne vesti interview)(WikiLeaks website). Each of these three organizations takes a different approach to the articles. AWP has local journalists associated with their local nodes write the articles (AWP interview). Juzne vesti itself is a media organization dedicated to investigative journalism and writes its own articles (Juzne vesti interview) WikiLeaks has global media partners that write articles about their releases (WikiLeaks website).

The article based on the release method works well for small releases, but large dumps of information are challenging. At the very least, big releases may require a
document tracking system like Document Cloud or the one WikiLeaks uses to manage the release of its media partners (“WikiLeaks setting another trap for journalists, NGOs”, 2012). Some organizations have experimented with crowd sourcing for analysis of large sets of documents. Public Intelligence tried crowd sourcing using a forum and failed to receive meaningful contributions (Public Intelligence interview). WikiLeaks has tried crowd sourcing as well, using the Twitter hashtag #wlfind for people to report their findings as they read through the cables and retweeting the responses. They have had some limited success with this tactic (@wlfind Twitter). AWP is currently experimenting with a crowd sourcing platform on the WikiLeaks Cablegate documents. This platform also includes a graphing tool for easy analysis of the connections between cables. It is not clear how successful AWP’s open source crowd sourcing platform will be at this point (AWP interview).

Release

All of the leaking organizations in the case studies put all or part of the document on their website at release. The exact form this takes varies. AWP and Juzne vesti post documents on their own news sites (AWP interview)(Juzne vesti interview). While AWP also posts the full leaked documents, Juzne vesti only publishes the minimum information needed to understand the wrongdoing they discuss (Juzne vesti interview). WikiLeaks and AWP both work with external media partners who may also publish an article at the same time as they publish the document (AWP interview)(WikiLeaks website). Public Intelligence and Cryptome both publish the leaked information directly on their websites and nowhere else (Public Intelligence interview)(Cryptome website).
Post-Release Actions

After release, most of the leaking organizations studied will do interviews, hold press conferences, or otherwise try to publicize their releases either voluntarily (WikiLeaks website) or on request (Public Intelligence interview). Juzne vesti may update articles if a wrongdoing is corrected (Juzne vesti interview). AWP goes a step further and hopes to mobilize their local nodes around issues presented in the release (AWP interview).

VI. Future Improvements

Overall, the current approaches for leak processing seem to work well for most small releases. For small releases, there are still ways leaking could be made easier so more people could setup and run leaking organizations. Organizations that seek to mobilize people in response to leaked material may also want to try new strategies for analysis. There has been some moderate success in mobilizing people in response to leaks but the situation could be far better. For large releases, new strategies for leak processing need to be developed. Big leaks face all the challenges of small leaks plus some. The best of the current approaches lead to long waits before release or release without redaction.

Automatic Metadata and Name Removal

A shocking number of organizations are still removing metadata by hand. This is not necessary. GlobaLeaks has discussed incorporating automated metadata removal into its framework. This is a very good idea and the metadata removal tools available should
continue to be expanded. Ideally, there could be an option for sources to remove metadata through the submission system before sending the leaked information.

Metadata is not the only thing that can be automatically redacted. Names could be automatically removed. WikiLeaks is the only organization that might be using automated name redaction. While such a system would not be perfect and documents should also be checked by hand, an rudimentary automatic redaction system would be fairly simple to make. Redaction software could be improved by using machine learning and natural language processing algorithms to better determine what to redact. This would drastically reduce the workload of leak processing in large releases. Automatic redaction could also be incorporated into the submission system so particularly cautious sources could redact names before sending the documents.

**Release Management System**

A customizable release management system could be useful for any leaking organization. At its most basic level, a release management system could manage filtering and categorization of documents received via email or a submission system and automatic formatting and posting of documents. Even Cryptome could benefit slightly from such a system. Other organizations may want additional features. When Associated Whistleblowing Press described such a system, they said "it should cover all the types of fields, be searchable through these fields, have commenting features and selection of different 'status modes' for each single file. Also, the ability to cluster files into pre-determined rules (by tags, keywords, field types, size, type of file etc)" (AWP interview). These features are all feasible to implement. Also, a system like the one WikiLeaks has for their media partners should be made publicly available. That would enable better
crowd sourcing and media strategies. A release management system like this could be created by altering existing free and open source tools that provide some of the necessary functionality.

Guide to Verification

Both WikiLeaks and the Associated Whistleblowing Press mention verification strategies they use but say that providing more detail would compromise their ability to verify documents. This is a form of security through obscurity and only puts up barriers to people who wish to create leaking organizations. Someone, perhaps an anti-forgery expert, needs to compile a guide on how to verify the authenticity of documents. Additionally, free and open source electronic verification tools should be created and perhaps incorporated into the release management system.

Study Crowd Sourcing Attempts and Failures

Crowd sourcing is an interesting approach to document analysis for large releases and a way to get people involved in the leaking process. Unfortunately, the current approaches have had minimal success. These failures need to be studied in more depth. Noveck provides some good suggestions for crowd-sourcing tasks like document analysis in "Wiki-Government" and these ideas should be more closely examined and tested within current systems. Additionally, an approach similar to AWP's local node system could be used to create more distributed leaking organizations. This may be more effective than traditional crowd sourcing practices. A distributed approach also reduces (but does not eliminate) the problem of leaking organizations as an extension of authority as power in the leaking organization is dispersed.
Graphical Analysis Tools

Graphical analysis tools like the one AWP provides for Cablegate could help with analysis or crowd sourced analysis as they help people understand the connections between documents. They could also be useful for document viewers who are trying to understand the content of the release.

Similarly, tools for placing documents in a narrative or identifying key points within documents could be added to a release management system to aid in the analysis process. Organizations like Public Intelligence who would like to provide summaries but limit their bias and let the viewers judge the document could use analysis tools to aid in objective summary construction. Other organizations that like to provide additional details could use such tools as a starting point in their analysis.

Test Release Method Effectiveness

How effective are leaks really? I have provided some assessment of their effectiveness but an in-depth study of leak reception and any actions triggered by releases should be conducted. Specifically, it would be interesting to see if sites following a minimal-processing strategy had more or less effective releases within the context of their goals than those who work with media partners and add additional information to the document. Is the outcome of the release actually that different?

Overall, it seems like most leaking organizations follow the same general process despite differences in transparency ideology. As a result, they do suffer from some of the same challenges. It is possible to address these issues by better understanding the
processes and challenges of leaking organizations. LeaksWiki provides a framework within which to examine leaking organizations and a start to this analysis.
Works Cited


Youssef, Nancy. "Officials may be overstating the danger from WikiLeaks Read more here: http://www.mcclatchydc.com/2010/11/28/104404/officials-may-be-overstating-the.html
M.C.: So I've looked at AWP some already but I was wondering if you could tell me a bit more about and its goals. Specifically, what would the ideal outcome of release of a set of documents be for AWP?

AWP: I think the main point of the AWP is the network structure. Even though we have an international focus, as in, we work on the Internet, we want to work with local communities. In this sense the ideal outcome would be a set of documents that could empower local actors to face issues in their communities. The point is that information on a local scale can be more powerful than on a globally, maybe more abstract level. By all that I mean that the outcome has to be an improved public control of institutions, accountability for their actions and so on...

M.C.: ah, makes sense

AWP: Like for example, massive releases make an impact on public awareness, but if the release is small but contains relevant information, it will have a definite impact on a local level... And by local I'm referring to anything from national level to cities, towns, neighborhoods, organizations or events (a period of elections, for example). And I guess the effect could be stronger as closer it gets to micro level hehe. If you can prove fraud during an election it will have a strong effect, for example.
M.C.: huh, that's interesting. Most leaking sites seem to be on the global or national scale but I've noticed a few on the local level. Since you work with local communities, how do you determine what will be relevant on the local scale? And do you work with people in those specific communities during the pre- and post- release process?

AWP: As we think in terms of network, each local whistleblowing platform (as we call them) is a node in the network and we are prepared to give them a certain level of autonomy. We understand that they are the most qualified people to discern what is relevant or not. Obviously our relation must always be based on trust. Right now we are preparing a node in Spain, first of all it will be national-level, although we have discussed making smaller nodes for certain activist platforms. The work we will always have to do with them is set up a functional working group: get them involved in the process and start building a network of people who will participate in moving the project around in the media (traditional and non-traditional), managing any information we receive, analyzing and publishing. Post release is an interesting question and we have different ideas on the method. Our hope is to incentive a collective response to any issues, depending on the scale of course. We have this idea of trying to bride the gap between news and action.

"but I've noticed a few on the local level." Which ones do you mean?

M.C.: I don't know how active they are and I haven't been able to reach them yet but there seem to be several country specific leaking sites and a few for major cities. I saw most of these on LeakDirectory, which seems to be down right now

AWP: Oh ok thanks for the tip, we're looking to collaborate and speak with other groups and so on.
M.C.: But I remember several leaking sites in Canada, a few in the UK, one in Israel, and there others too. Most were country specific but there were a few for major cities, the one that comes to mind first is BaltiLeaks. I'm not sure how active all of them are though.

So generally do you or the local nodes initially receive leaked info? Or both?

AWP: Ok, will investigate. I think we know who is listing on LeakDirectory, we'll ask. All info goes straight to our central servers and then we share the info for analysis. The people we trust the most in each node will help with verification and with organizing a team for analysis.

M.C.: ah, okay. And after you receive info what steps does it generally go through to prepare it for release?

AWP: We have a set of basic data management policies which will be found constantly in all our sites, before submission etc. Every node has to follow these guidelines even though they are essentially self-organized and relatively autonomous. Basically we state that we'll only accept material that serves to prove corruption and abuse, that is no first hand accounts or rumors. Afterwards we have to verify the material working with the nodes, considering possible forgery, use, reason or cost for faking information. We'll ask for external opinions if necessary. Then we have to redact certain information to protect violating people's privacy, if they appear in the information and are unrelated for example. We also have to clean the files' possible metadata - for source protection etc. Then analysis, which ideally would be done in a hard news format: when, where, why and so on and publishing through our media contacts. You have a full version of these policies on our site if you want to read them

Part Two
M.C.: Your website mentions that you cross check documents and gives some of the things you consider (motivation for forgery) but is there any consideration not listed there? And generally what tools or techniques would you use to verify its accuracy?

AWP: You mean considerations strictly related to cross-checking?

M.C.: cross-checking or verification of documents authenticity

AWP: There are both conceptual tools and electronic tools. Conceptual cross-checking means detecting the accuracy of the document regarding historical facts, actors and their behaviours. Although the central node of AWP provides guidance on this type of cross-checking, it is a work to be done by the local working-groups. Our feeling is that local community is more prepared to detect, conceptually, whether a submitted material is accurate or not.

As for electronic cross-checking, there are tools to and practices in order to detect the authenticity of scanned documents, photos and videos. This is a work mostly to be performed by specialists in the field of forgery, who we are in contact with. But actually I consider that the most relevant and decisive task regarding cross-checking is performed in the conceptual checking, since there is a point were electronic forgery is almost perfect.

There are also some ways of cross-checking which are performed after the document is published.

M.C.: ah, what are those?

AWP: It happens when the part affected by the leak publicly stresses that the information is authentic, directly or indirectly.

M.C.: ah, right, like if you get a request by the organization it was allegedly leaked from to take it down?
**AWP:** Not only a request directly sent to us, but there are cases when organizations publicly admit that some of their classified information was leaked.

**M.C.:** Do you have any way the people looking at the document can tell if an organization has done this or if it got past electronic and/or conceptual cross-checking?

**AWP:** Sorry, can you re-structure the question?

**M.C.:** Sure. If someone is looking at a document, could they tell if an organization has said directly or indirectly that the information is authentic? Or if it got past your cross-checking?

**AWP:** We will only release documents which passed by our standards of cross-checking. So if the document is published by us, it will be implicit that it passed by our cross-checking. As for confirmation from the organization where the document was leaked from, we shall point out this confirmation in the same 'release page' of the document. Documents will have a 'front page' where this kind of information will be displayed. The 'cross-checking seal' of the AWP and possible information about organizations' confirmation of authenticity.

**M.C.:** ok, great. So how do you clean up metadata from different types of documents? What tools do you use to do this and do you have to do parts of this by hand?

**AWP:** This kind of information we are not able to disclose publicly since it could facilitate forgery. But there as several methods of 'metadata cleaning'. Most of it is indeed manually done.

**M.C.:** ah, okay. I was wondering if it was automated if there might even be a way to do it before the document is sent.

**AWP:** There are tools available on Internet which could be used by potential whistle-blowers, indeed.
That is also an idea that we could implement

**M.C.:** You mention a two-part analysis step on your website. How long does each part of this step take? And how much does it vary between different types of releases? Also, is this done primarily by the local groups or AWP?

**AWP:** Part 1 strictly depends on the kind of batch. It takes longer as bigger the batch is, since it consists on classifying and tracking the batch. Part 2 is about news-making and should take 'standard' time of writing a journalistic piece. Some journalists take months preparing an investigative piece, others can take 1 or 2 days. As for what we are going to publish in our newsroom, http://whistle.is, will be 'hard-news' which usually take no more than 2 days per subject.

As for how long media partners will take to write a piece, we sincerely can't tell. We are studying ways of providing crowd sourcing tools where journalists and public can investigate and publish together on big batches.

**M.C.:** ah, have you found anything useful in crowd sourcing so far? I've been wondering about how viable that is for a while

Also, is it mostly the media partners who do the second part of the analysis step?

**AWP:** We are going to launch a tool for crowd sourced Cablegate analysis and newsmaking this week. We plan to have it as a study-case which could be implemented to other databases and batches in the future. Yes, tools are still to be created, since all this is really new in terms of historicity.

- dont publish it before 28nov 2012 *** http://cablegate.awp.is

**M.C.:** ok

oh wow, that looks interesting
**AWP:** we are still fixing minor bugs, text and presentation as well as increasing the database. But that is the major idea.  

**M.C.:** I'll definitely be keeping an eye on that to see how it goes. The main other similar site I have seen is Crowdleaks but that looks like it is also under development.  

**AWP:** Yes, unfortunately. I never saw Crowdleaks really in activity. You might find it interesting as well. This is the graph tool we will have attached to each cable in the cablegate tool. This graphic is the graphic for 08beijing3055 for example:

http://194.150.168.63/cab/08BEIJING3055.gml.html  

- last link must be opened with Opera browser or latest firefox*  

**M.C.:** Do you ever remove/redact names or other information from documents?  

**AWP:** Yes, we redact all information regarding third parties which are not directly involved in the wrongdoing to be reported in the document.  

**M.C.:** Is that done manually when you first read through the document in the first part of the analysis step?  

**AWP:** Yes, exactly. Depending on the batch, i can be done in the second part as well.  

**M.C.:** So, just to be sure I have this right, the steps you typically go through after receiving a document are conceptual cross-checking, electronic cross-checking, removal of metadata, read-through for large sets of documents, analysis of documents and redaction in this step or the previous one, and publication on the news wire? And most of these steps with the exception of electronic cross-checking and potentially some metadata removal are done by hand?  

Oh, also, do you use any system for tracking which documents have been read or analyzed in the analysis step?
AWP: Yes, I think you understood correctly. But there are cases and cases. It does not mean that we are going to analyse each file separately in each batch. For example, we receive 10gb of e-mails of a certain organization. We won't cross check all of them, we will cross-check the database as a whole.

M.C.: That makes sense. But doesn't removal of names get tricky there because someone not related to the wrongdoing could easily be mentioned in such a large database of emails?

AWP: Systems for cross-checking/analysis tracking are also still to be created and should fit specific need according to each batch or database they cover.

M.C.: Ah, ok. Could you go through what features might be most useful for a few different types of batches or databases?

AWP: It's complicated. I could send a mail with a list :-)

But basically it should cover all the types of fields, be searchable through these fields, have commenting features and selection of different 'status modes' for each single file. Also, the ability to cluster files into pre-determined rules (by tags, keywords, field types, size, type of file etc).

M.C.: Ah, okay. If you get a chance an email with a list could be useful at some point also, since you mentioned large databases of emails, what if some of the emails pass your moral policies but others do not or are not significant? Would all of the emails be published or just some of them?

AWP: Just some of them.

Although electronic (and in some cases conceptual) cross-checking can be done massively, documents are considered individually when it regards to moral policies.

M.C.: Ah, ok
M.C.: How would you define leaking and whistleblowing? Do you think of them as synonyms or different things? And how does AWP fit into that definition?

AWP: Leaking and whistle-blowing originally are not the same thing. Recently, tho, these practices are getting closer to each other when it concerns to public opinion. I wrote something here that could be useful to understand: http://whistle.is/?p=283. Originally leaking should be simply 'the activity to make secret information be publicly accessible' and whistle-blowing the 'ethical leak', it means, leaking with the purpose of revealing wrongdoing, crimes, corruption etc.

AWP is a media agency focused on 'whistle-blowing'.

M.C.: thanks! So I know AWP is fairly new. Have any of your local nodes released documents yet?

AWP: We currently have only 1 node, although the plans are to expand it during the next 2 months. This node, the Icelandic one, created 57 days ago, did not release files yet.

M.C.: ah, okay. I'm interested to hear how it goes when it does. Are there any tools that you don't have or don't exist now that would be helpful for you in processing documents? What would these be? And you mentioned some tools for metadata cleaning and cross-checking- could you tell me if these are free and open source or not? Also, is your crowd sourcing platform free and open source?

AWP: Our crowd sourcing platform for the Cablegate files is free and open source. As for the rest, can I think about it calmly and send to you by e-mail? Do you have a PGP/GPG key?

M.C.: Sure. And http://pgp.mit.edu:11371/pks/lookup?search=Shidash&op=index the top one there is my key (7F063537)
And I think that is all my questions unless you have anything you want to add or any questions for me

**AWP:** I think that is ok for now

thanks for getting in touch :-)

---

*Cryptome Interview*

**M.C.:** What is the ideal outcome of the release of a set of documents for Cryptome?

**Cryptome:** That many other persons will disclose sensitive and informative documents and other forms of publicly accessible, non-secret information: video, recordings, images, talks, conversations, whisperings, singing, yodeling, drum beating, sign language, body gestures, dance, paintings, drawings, sculpture, graffiti, samizidats, leaflets, protests, insults, fist fights, traffic blockage, defiance of all open and secret forms of authority in unexpected and unprecedented ways, again and again, never-ending, alone and in cooperation with another, with groups, with crowds, with mobs, with militants and angry suburbanites and workers, with anybody with a grief unanswered, avoiding leaders of all stripes, and bosses and organizers and funders and leeches and exploiters and ideologues of self-serving deviousness, in particular those with with socio-econo-political agendas concealed by lying promises, secrecy and backed by backroom out-of-sight shenanigans and the deadly force always required by authority to screw the public with innumerable, incomprehensible taxes, high profits, pocketpicking tithes, panhandling donations. And a lot more coming and growing and getting wilder along those lines which have been around since humans rose from the slime to brain-wave means and
methods to dominate and cheat, kept in check only by those willing to reduce the dominators to pulp manure.

M.C.: What process does a document or leaked information go through before being posted on Cryptome and what are the goals of each step? I am interested in the whole leaking process but particularly focused on steps done between receipt and release of the document like verifying the document, removing people's names, adding context, etc. What are the most time consuming and/or difficult parts of this process?

Cryptome: Not much. If a document will annoy, and best, deeply anger, believers in authority then it gets published. Leaking is just one way of doing that. Far better is to provide documents and disclosures and oppositions and protests that are not dramatic leaks but encourage others to share information of all kinds to buck authority and drive it insane with fear of insignificance and uselessness, and most terrifying, dead broke facing hard labor like those they exploit.

We prefer libraries over leakage in which leaks may be implanted but are not the primary goal. Leaks are a publicity gimmick, all too often a form of authority closely imitating media to bedazzle consumers, while libraries foster self-education and criticism and if all goes well, thoughtfulness rather than addictive adrenaline of leaks and infantile headline spoonfeeding. (Leaks like pablum were invented by authoritarians to attack and dumb-down others to their low-level with manipulative, biased screechings.)

The most time consuming is formatting for publication, but it is not that difficult, takes far less time than reading news media, watching TV and movies, games playing and weight lifting, putting on make-up and preening, shopping and eyeballing useless products. About the time it takes for daily bathroom activities, excluding manic self-pleasuring.
We occasionally remove names but not if they are supporters of authority. Hint, leakers and leak sites are authorities in sheep's clothing. The biggest and most prolific leakers are authorities leaking openly and covertly through the press, through NGOs and academics, through shills and authors, through allegedly ex-authorities, through phony dissidents, by any means to manipulate public understanding and behavior, and make a buck and keep taxes coming in.

**M.C.:** Do you use in any particular tools in processing documents received? Examples could be tools to remove metadata, manage the review of documents, etc. If so, how well do these tools work? And are there any tools that could make the process easier?

**Cryptome:** No tools beyond what any computer user has. All done by hand, no automatic programs -- these are not reliable and are based on an authority model like most labor-saving devices to induce sloth and thoughtlessness. Mass production is authoritarian and its promotional material exactly the same. Big numbers and big data are big deceptions to avoid public, personal, face-to-face accountability.

It is cheap to run a disclosure site, nearly anyone can do it on pocket change. Don't believe the nutty claims of needing large donations, that's the high-profit model pushed by commercial media, fat NGOs, moneymaking education and religions, and incurably verbose and scribbling hustlers vomiting branded messages of public benefit (LSoS) indistinguishable from governmental and commercial cohorts padding one another's purse with tax favoritism, bribery, PR, swapping slobber at feasts in off-the-record salons inside the manifold global beltways funded by financial theft centers -- the giant foundations aggregated in the paper New York Times today in a two-page braggardy serving as recovery refuges for retired scoundrels from gov-mil-com-edu-ngo.
M.C.: Aside from you and the source, are others involved in helping with the leaking process? What parts of the process do others generally help with? And is the source ever involved in the process beyond the initial submission (for example, by providing additional background information or helping with verification of documents)?

Cryptome: Sources are the heavy lifters, thousands of them busting their chops for whatever reasons they have to provide information, we do little by comparison. We do not believe in "context." That is authoritarian nonsense. For the same reason, we do not believe in verification, authentication, background, foreground, advertising, promotion, branding, corporatization, any form that enlarges the gap between individuals and those who claim to protect them, educate them, save them from the devil, advocate national security racketeering, supports official, secret spying at home and abroad.

M.C.: Do you think of leaking and whistleblowing as synonyms? How would you define each of them (or one of them if you think of them as synonyms)? And how do you think of Cryptome in terms of leaking and whistleblowing?

Cryptome: Monetized leaking and whistleblowing, like exposes and documentaries, are publicity terms among a slew of other less melodramatic disclosure methods. They have come to be brands that diminish the less well-known initiatives which are more pervasive and available for wide use by non-authoritarian, non-monetized efforts. Cryptome is a place to exchange free material among thousands of others like it, before, now and in the future. Nothing special about it. And by no means trustworthy, quite the opposite, suspicion encouraged. Do your own, without delusion of models to follow. What do you think, come on, out with your villainous media. MIT-driven, government and corporation mega-funded agenda, you "fucking spy."
Juzne vesti Interview

Part One

M.C.: What is the ideal outcome of the release of a leaked document and/or an article based on a leaked document for juzne vesti?

Juzne vesti: I am not sure that I understand question? In general, I am always happy when government officials have to react :)

M.C.: Could you explain the steps a leaked document goes through from receipt to release of the document or an article based on it? What are the most time consuming or difficult parts of this process? Do you normally release documents or leaked information with the related articles you publish?

Juzne vesti: in basic, when we receive scan of some document we are using FOIA to ask for that doc from official source. Sometimes journalist would just call some official person and ask for comment. If that person, through comment confirm that doc exist, we can procede.. in other way, we will use FOIA :))

Anyway, there is no way that we will publish unchecked document. Everything we receive we see only as a clue, nothing more.

M.C.: Do you use any particular tools when processing leaked information or documents? For example, tools to remove document metadata or verify information. If so, how well do these tools work? And is there any tool that could make the process easier?

Juzne vesti: Perun is removing metadata by default before it send it to us. So, there is no need for that further.

Part Two
M.C.: On the first question, I guess it could be rephrased as- what is your goal when releasing documents or why do you release documents? Some sites do it to increase transparency generally, others to identify wrongdoings, some hope to correct and/or raise awareness of wrongdoings. Have government officials ever had to react from a release of yours? If so, could you tell me a little more about that case?

Juzne vesti: aha, now I understand :) I think the most logical answer would be "all mentioned" :)) The cause I have founded Juzne vesti was my disappointment because I could not find a media that will publish my investigative storie about some illegal procurements on city airport, in witch both city and state government were included. In that time my goal was to inform citizens, tax-payers, that somebody is stealing their money. Off course, personaly I was happy when prosecutors office had started investigation after my article was released in JV, and even now, 3 years latter, the tiral continues.

In general our goal is always to rise awareness of citizens about their rights, but depends on case we expect some reaction from officials - that can sometimes be prosecutor, sometimes magistrates court, mayor,.. or even public company that will solve some municipal problem.

Let me give you a few examples:

- We have published the story that the brother of mayors chief of stuff started working and immediately become chief in one city owned company, but there was no any public contest for that positition. It is important to metion that new mayor was elected in mid July, and one of his key argument was "there will be no political employments in public sector". Day after we have published article, mayor released statement that his chief of stuff brother was fired.
- After Juzne vesti released article that city owned building directorate have just published contest for pawing 5 streets that were already been pawed (unofficially, they have hired one building company to paw streets, but without contest. So, they had to publish contest later to try to cover everything), Directorate have canceled the contest.
- We have published article the general manager of city owned heating plant (the only one in city) had hired her son and daughter of her assistant, and give them chief positions. 7 days later she was fired.
- Only few hours after we have published article about some road sign that was placed on sidewalk in the middle of track for blind, that sign was moved.

But, unfortunately, it is not always this "good".

At the end, let me conclude - we always have few goals - to force public officials to fix wrongdoing (or to stop), to increase transparency generally, and to raise public awareness on the topic. It is hard to separate those things.

M. C.: Do you ever verify documents in ways other than getting it through FOIA or having an official comment? Around what percent of the documents or info you receive can you verify?

Juzne vesti: Of course. Etc, for the story about heating plant (director hired her son), I have received information in Friday, few hours after she had signed the contract and guy should start to work from Monday. I did not have a time to send FOIA (they have 15 day to answer, but if they don't I have to appeal to Commissioner and whole process last at least 2-3 months), so I have called director and I said to her that I have those contracts (I was lying, I only had information about them), and asked her for comment and she can confirm me the authenticity.
She said that she don’t want to comment but have offered me to come to her office during next week and she will show me contracts - that was enough for me - indirectly she had confirmed that contracts exits :)

M. C.: After verifying documents, do you do anything else to them like remove names? If so, what? Do you specifically look for evidence of wrongdoings in the documents and information you receive?

Juzne vesti: We are trying to be careful about personal data. Public official name is not personal data, but his address and date of birth are, so if we are publishing that document we are covering that data with black colour.

http://www.juznevesti.com/uploads/assets/2012/10/17/18157/800x600_kpd-putni-nalog-napomena.jpg - from article about some broken vehicle from city prison which was "spending" gasoline (according to documents).

M. C.: Do you publish all verified information? If not, what are the standards you use to determine what to publish?

Juzne vesti: I am not sure I understand question. In general we are free to publish all verified informations, but we publish only those that we think it is important for citizens to see. That means if we have 100 pages of some contract, we will publish only the one that is directly related to article.

But, I am now sure this is what you wanted to ask.

M.C.: When you do publish documents or information, what information do you post it with, if any (for example, background information or context, related documents, highlights of potential evidence of a wrongdoing)?
**Juzne vesti:** If we have them we publish everything we think it is important so readers can have a whole picture. Sometimes it is a photo, sometimes scanned document, and recently more often audio or even video.

**M.C.:** How many people generally help with reviewing and processing documents and information? Are these primarily journalists involved in juzne vesti? Have you ever asked for more information from the source (and do you have an anonymous method to do so)?

**Juzne vesti:** yes, primarily that is on journslist to do, but we now have a good "pool" of consultants - from former Supreme state auditor, former prime minister, former mayors,.. off course, if we need to publish some statement, we are mostly mentioning the name of source. It may sound a little irrational, but from time to time we are publishing comments from current mayor or tax office director, but as "anonymus source" - which means sometimes they are our whistle blower. This is happening when they are personaly against some cause, but majority in their political party thinks different. If we think that his (mayors) standings is wright, we will signed him as anonymus - off course, this is very rare and we are always have their statement recorded in case we have to go to court. This can be a matter od code of etic, but I am just saying how we works.

**M.C.:** Do you think of leaking and whistleblowing as synonyms or different terms? How would you define each of them (or one of them if you think of them as synonyms)? And how do you think of Juzne Vesti in terms of whistleblowing and leaking?

**Juzne vesti:** hmm.. I personaly see whistleblower as person who believe in justice and is blowing in whistle to alarm on some wrongdoing, now expecting special reward for that. On the other side, leaking can be motivated by some other goals (political, social, economical,..), but, it is a matter of definition in each country. In Serbia we still do not
have a word for whistleblower. We are curently using word "uzbinjivač" which in literall means "the one who started the alarm"..

From my perspective, I do not care who gave me information if it is correct, not false. Sometimes we receive info from political opponents, sometimes from ex-girlfriend.. but, when I have some documents in my hands that are showing some ilegall stuff, I have a story. Off course, if "source" is asking from you to do story under some conditions (such as "not mentione me in story" and so), we are alwaly having a discussion on that.

Part Three

**M.C.**: What is the hardest part of the document and information processing, leaking, and release process? What is the most time consuming part of the process?

**Juzne vesti**: Depends on situation. Usualy it is collecting the statements of peoples we are mentionig.

**M.C.**: Are there any tools that might make document processing easier for you? What would these be?

**Juzne vesti**: hmm.. no.

**M.C.**: Is there anything else you want to say or tell me about Juzne vesti?

**Juzne vesti**: We have started experimentaly work in August 2009, but official start was in Januar 29th 2010. In that moment we had 3 journalists, now we have 12 and lot more that we are cooperating with. We have 22-24.000 visits per working day (on weekend we have 40-45% less visits per day), and monthly rise of more than 15%.

All members of our team are younger than 35, and avarage age is 27.
Among daily news, we are focused on topics related to corruption. I believe that we have become recognizable because of that -http://www.youtube.com/watch?v=HHBvyM0k8ek&feature=youtu.be&t=20m57s

I wish you all luck with your work, and I would be happy to see results of it :)

Public Intelligence Interview

Part One

M.C.: What is the ideal outcome of a release of a document or set of documents for public intelligence?

Public Intelligence: The ideal outcome is simply to do justice the material being presented. Our particular intent is not to force transparency on anyone, but simply to inform people. We feel that access to information is a fundamental human right, allowing individuals and societies to orient themselves, make decisions and have some modicum of control over their own lives. Thus, our only intention in publishing a document is to provide the material to the widest audience possible, presenting it in a manner that is clear and straightforward so that readers can understand and benefit from the information that it conveys.

M. C.: Could you walk me through the process your documents go through from when you receive the documents (or even before) to release of the documents? I am interested in the whole leaking process but particularly focused on document processing steps like verification, removal of names, analysis of a document, etc. What are the most time consuming and/or difficult parts of this process?

Public Intelligence: The majority of the material published on Public Intelligence is, as the name implies, obtained from public sources. The purpose of the site has always been
to make information more accessible to people by aggregating original source material from the public sphere that is restricted, censored or otherwise difficult to obtain. This means that we often know the source of a document directly because we obtain the documents ourselves and can thus determine their authenticity, provenance and purpose by understanding the nature of the source from which we obtained them.

Once a document or other information is acquired it is reviewed to determine its relative value and whether more thorough analysis is warranted. The intensiveness of this process varies from document to document based on a number of factors from personal interest to the availability of time. However, the function of our analysis is always aimed towards making the material more accessible to people by elucidating key points or other useful pieces of information that the document may contain. We do not want to function like an intelligence agency or a major media company as these forms only further the current system where information is wielded by institutions to benefit a few, rather than benefiting all. The most important function that we can perform is simply to get the information out to people. They must create context, meaning and relevance for the information themselves.

We almost never perform redactions to a document, as this too would defeat the purpose of making information freely available. The only circumstances where we have done so is to remove intensely personal and/or legally protected information that serves no educational function, like a person's social security number. We also have, on a few occasions, performed redactions to ensure that the source of a document is not discoverable. Over time, this allows for more information to enter into the public domain than if we were to simply post the document with nothing removed.
The most time-consuming part of this process is always the acquisition of material that is worth publishing. People are rarely, if ever, going to risk their lives and/or livelihoods to come and drop material in your lap. This is one of the things most people don't understand about so-called "leak" sites: they receive far fewer "leaks" than you would imagine.

**M.C.:** What tools or software do you use throughout the leaking process and for what? How well do these tools work? Are there any tools or improvements to the tools you use that could make the process easier?

**Public Intelligence:** We try to incorporate free and open source software as much as possible into the publishing process. This is intended to demonstrate the degree to which people with minimal technical experience and small amounts of money can operate publishing platforms capable of disclosing information and helping to inform those around them. So, we use Wordpress to publish the site and other free software for communication, encryption and similar functions.

**M.C.:** How many people generally help with document processing? Do you ever ask experts in the area relevant to the documents to help with analysis? Have you ever tried to crowd source any part of the leaking process? Have you ever worked with media partners? If so, what sort of media?

**Public Intelligence:** Not many. We don't provide the documents we obtain to experts because this would defeat the purpose of our project which is to provide information to the public, not create a cartelized collection system for profitable media companies. We have tried to crowd source parts of the analysis of documents, but have found that it is difficult to attract individuals who are willing to contribute meaningfully. We have never provided documents to media outlets or reporters prior to their publication on our site. At
times, we have discussed material with reporters who had questions about its provenance or implications. This can sometimes be an intensive process.

**M.C.:** Do you think of leaking and whistleblowing as synonyms or different terms? How would you define each of them (or one of them if you think of them as synonyms)? And how do you think of Public Intelligence in terms of whistleblowing and leaking?

**Public Intelligence:** I don't really like either term. Leaking sounds like an accident and is a favorite tactic of those in government. Whistleblowing sounds like something done by a hall monitor in grade school. Telling the truth shouldn't require special terminology. We should endeavor to build a culture that is built upon truth-telling and openness, rather than one that lauds these activities as praiseworthy or unusual in nature. Public Intelligence publishes information that is of value and then tries to defend that information from attempts to censor it. That is all. Call it what you will.

**M.C.:** How effective has Public Intelligence been in achieving its goals and ideal outcomes with release of documents? What are or have been the main obstacles to achieving your goals? Is there anything that has or could help Public Intelligence be more effective?

**Public Intelligence:** We have had tremendous success in our primary purpose: to publish information of value that is difficult to acquire or not otherwise publicly available. In fact, we do this on a daily basis. The problem comes in trying to get people to pay attention to the material. We struggle often with how to make complex material accessible and relevant to audiences that are not necessarily motivated to understand it.

*Part Two*
M.C.: You mentioned that you tried to crowd source parts of document analysis. What parts did you try to crowd source and how? Did you have any success or was it just too difficult to find people who would contribute?

Public Intelligence: We tried to aggregate readers' efforts to find interesting material in a set of documents from NATO and the UN regarding the war in Afghanistan. We used simple, publicly available forum-based tools to try to do this. But, not many people ultimately contributed.

M.C.: How do you determine the value or significance of a document?

Public Intelligence: There are a number of factors in the appraisal of material that are difficult to articulate, but they generally revolve around the public worth of a document. Does the document describe or reveal something about a public process? Does the document relate information that is informative or educational in a broader societal context? Who produced the document and what are the rules/laws governing its disclosure or publication? Has someone else already published the document? Does the publication of the document contribute in some way to the body of available information on a topic of public importance? These are some of the questions that might be asked.

M.C.: Do you have any particular guidelines or practices you follow during analysis? For example, how do you avoid imposing context while still making the information accessible?

Public Intelligence: We do what good journalists are supposed to do: explain the material in a manner that attempts to limit our own personal biases. Sometimes we are more successful at this than others. Journalism/leaking/disclosure/whatever you want to call it as much an art as it is a craft.
M.C.: Have there been any releases people have paid more attention to than normal? To what extent do you think the attention the material receives is due to the analysis and accessibility versus the nature of the content?

Public Intelligence: In the thousands of documents we have published since we began doing this several years ago, hundreds have received coverage in various types of media all over the world. However, the most popular stories are always the ones that are most marketable due to some salacious or attention-grabbing quality, not necessarily their true informational value. For example, we published a document and an article earlier this year on an IARPA program called Catalyst that is designed to act as an "entity extraction" and "semantic integration" system across the entire intelligence community. The system is designed to parse large-scale datasets and automatically extract and organize meaningful information for storage and analysis in later investigations or intelligence gathering. It's a dry topic, but has tremendous implications for a number of issues like widespread electronic surveillance. Basically no one paid any attention to this. On the other hand, a few months prior we got a story into the mainstream media that was so popular that it was reported everywhere from Indian TV to Good Morning America. It was about how apparent gibberish in an early version of an al-Qaeda magazine was in fact cupcake recipes. There were headlines like "Al-Qaeda Mag Attacked in Operation Cupcake." That should give you an idea of what I'm talking about.

M.C.: Do you use any tools internally for tracking documents you are analyzing or otherwise waiting to release? If so, what tools? Similarly, do you use any software to aid in your analysis process? And is there any software or tool that would be helpful in your analysis process?

Public Intelligence: No, not really.
M.C.: Generally, how do you obtain your information? I don't want information on specific sources but you noted that you obtain the documents yourselves so am interested in how you get difficult to obtain or restricted material.

Public Intelligence: It's all around, you just have to look for it.