WIKILEAKS: IMPLICATIONS FOR STATE CONTROL OF INFORMATION

JUDITH REPPY

CORNELL UNIVERSITY

JANUARY 2012

OVERVIEW OF THE ARGUMENT

Legitimacy in democracies depends on transparency in government.

All governments have secrets, but only some are legitimately kept from the public.

The Internet, along with huge databases, has created vulnerabilities in secrecy regimes.

The ability of states to maintain control of information is still considerable, but constrained.

Case study: WikiLeaks

THE NEW INGREDIENT: LARGE DATA CACHES

Organizations at all levels of society have created data bases to take advantage of the Internet as a means to store and share information.

They are deeply embedded in organizational practices at all levels.

Thus, a certain vulnerability is unavoidable. It can be managed, but not eliminated.

WHAT IS WIKILEAKS?

A not-for-profit, web-based organization launched in 2007 by Julian Assange and colleagues to provide a "secure and anonymous way for sources to leak information" via an electronic drop box. After review by an editorial board, the data are published on the WikiLeaks web site.

Note: Assange and the organization identify themselves as journalists.

RADICAL TRANSPARENCY

The ethos of WikiLeaks is full transparency:

"The broader principles on which our work is based are the defence of freedom of speech and media publishing, the improvement of our common historical record and the support of the rights of all people to create new history. We derive these principles from the Universal Declaration of Human Rights." (WikiLeaks.org, "About")

MORE ON WIKILEAKS

The technology involves encrypting the files received and re-routing them, using standard tools to protect the identity of the leaker. The web site is based in Sweden, a relatively safe haven.

WikiLeaks' claim to preserve anonymity seem justified; where leakers (e.g., Bradley Manning) have been identified, it was not through WikiLeaks.

MULTIPLE ACTORS

WikiLeaks is a network: it takes several different kinds of actors to move information from the secret domain to the public domain:

- Someone with access to the information and a motive for revealing the secrets.
- Someone to receive the data and publish it.
- News media to spread the story.

HACKER, WHISTLEBLOWER, JOURNALIST— SPY?

In the age of the Internet, there are new players providing information to the public. Legacy media have been joined by other sources—e.g., blogs, crowd sourcing, fact-checking sites.

Assange has been a hacker, whistleblower, and journalist, but he is not a spy. Nevertheless, some members of the US government have called for his prosecution under the Espionage Act.

FROM OBSCURITY TO NOTORIETY

Early WikiLeak stories had limited public impact.

The 2010 Bradley Manning leaks created a media frenzy. They included:

- **Video “Collateral Murder”**
- **Files on the conduct of the Afghanistan and Iraq Wars.**
- ***Cablegate*: 251,287 US diplomatic cables.**

COOPERATION WITH LEGACY MEDIA

For the US leaks, WikiLeaks initiated a collaboration with mainstream media.

Purpose was to insure widespread publicity for the stories by offering exclusive first access.

Other motives:

- help in the task of review and redaction of files
- a mantle of legitimacy from association with mainstream newspapers

BREAKDOWN OF THE PARTNERSHIP

Inherent tension between WikiLeaks' roles as a source for leaked material but also a competitor in publishing.

The collaboration broke down over personality clashes and refusal of the Guardian/NY Times to regard WikiLeaks as anything more than a source.

The sincerest form of flattery: The WSJ and Al Jazeera have opened their own secure drop boxes.

WHISTLEBLOWER—AN AMBIGUOUS CATEGORY

Df: a person who tells the public or someone in authority about alleged dishonest or illegal activities occurring in a government department, a public or private organization, or a company.

Whistleblowers enforce a kind of accountability in situations where actions otherwise go without scrutiny.

Bradley Manning: Hero or traitor?

A RISKY UNDERTAKING

There is a high risk of retaliation—shoot the messenger. One NGO titles its advice handbook "*Courage Without Martyrdom: A Survival Guide for Whistleblowers*"

In the USA and some other countries, there are laws to protect whistleblowers against reprisals, but only if certain conditions are met. In most countries there is no protection.

HOW CABLEGATE WAS POSSIBLE

SIPRnet is the worldwide US military internet system, separate from the ordinary internet.

Dispatches marked SIPDIS were automatically downloaded to the embassy's classified website. Up to 500,000 people had access—anyone in the State Department plus anyone in the US military with a security clearance up to the 'Secret' and a computer connected to SIPRNet.

The DOD did not monitor usage or limit downloads to external devices.

SECURITY AT CAMP HAMMER, IRAQ

Bradley Manning's description:

"Perfect example of how not to do INFOSEC [information security] … pretty simple, and unglamorous… weak servers, weak logging, weak physical security, weak counter-intelligence, inattentive signal analysis … a perfect storm."

U.S. GOVERNMENT RESPONSE TO CABLEGATE

DOD introduced real-time monitoring of large downloads from SIPRnet.

It blocked use of external devices in most computers and introduced smartcards in place of passwords.

The State Department cut its link to the secret level of SIPRnet.

Federal employees were ordered not to read the leaked cables.

RETALIATION AGAINST WIKILEAKS

Government officials put pressure on financial institutions to block donations to WikiLeaks, e.g., by declaring that it was an illegal organization in the USA.

PostFinance, Amazon, PayPal, Visa, Mastercharge all severed ties with WikiLeaks.

Internet service providers were pushed to terminate services to WikiLeaks.

RESILIENCE

WikiLeaks was able to use the redundancy in the Internet infrastructure to find new servers and back-up payment arrangements.

Nevertheless, it suffered a huge drop in donations, and had to close down last fall for several weeks.

These events show the downside of private ownership of the Internet infrastructure.

RETALIATION AGAINST ASSANGE

A Grand Jury was empanelled to review evidence to indict Julian Assange.

Legal basis for this is iffy: Assange is not a US citizen and he operates outside the USA.

Government lawyers requisitioned email and twitter accounts of people associated with WikiLeaks.

These actions contravene European privacy law.

RETALIATION AGAINST ASSANGE

If a link to Manning is proved, Assange might be indictable under conspiracy laws.

Such an indictment would raise serious issues for press freedom. In many cases, reporters give encouragement to would-be leakers. Where do you draw the line?

CONSEQUENCES OF CABLEGATE?

The State Department was embarrassed and had to devote large resources to apologizing for the breach of security and the content of some of the cables.

Hilary Clinton described her January 2011 tour of Middle Eastern states as an "apology tour," and said "I think I will be answering concerns about WikiLeaks for the rest of my life, not just the rest of my tenure as Secretary of State."

CONSEQUENCES 2

Some claim that Cablegate was a game-changer for U.S. foreign policy.

Secretary of Defense Gates, however, disagreed: ". . .some governments deal with us because they fear us, some because they respect us, most because they need us. We are still essentially, . . . the indispensable nation. So other nations will continue to deal with us. They will continue to work with us. We will continue to share sensitive information with one another. Is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. foreign policy? I think fairly modest."

OTHER CONSEQUENCES

State Department officials were seen by and large to be conducting themselves well and in accordance with US stated policies.

In Tunisia, the leaked cables were reportedly a spur to the uprising that began the “Arab Spring.”

In the USA, the clampdown on information exchange and proposals in Congress for new laws may result in less transparency, not more.

LIMITS TO STATE POWER

Self-imposed limits:

In the USA, the First Amendment has been interpreted to protect journalists who publish information passed on to them by others, even classified information.

Extradition treaties limit the types of crimes covered. In general “political offenses” are excluded. Whistleblowing is a pure political offense.

LIMITS TO STATE POWER

Limits beyond the legal framework:

The Internet is so large, so decentralized, so global, and so important to states and societies that direct control of it is not feasible. Even China, which exercises broad censorship controls, can not completely block access to the outside world.

The insider threat cannot be eliminated.

CONCLUSIONS

Leaks will happen again, even if all the proposed technological fixes are applied.

A leak on the scale of Cablegate is less likely (until the next time it happens).

The fall-out from Cablegate on US national security appears to have been small: Gates is right.

The fall-out for US foreign policy even smaller—a missed opportunity.

CONCLUSIONS

WikiLeaks, the organization, may or may not survive its legal and financial problems, but the model for handling large scale leaks anonymously is available for others to use.

Current US law will probably protect Julian Assange from prosecution in the USA.

CONCLUSIONS

Future legislation as proposed in reaction to Cablegate would, however, create new penalties for leaking government information to the media and reduce the exchange of information within the government.

Extra-legal pressure by the government on vulnerable private institutions is an unsolved problem.