Secrecy/Classification & Radical Transparency for Chinese Learners

This handout is intended to aid discussion of documentaries like *We Steal Secrets* (2013, about Wikileaks, Julian Assange, and Bradley/Chelsea Manning) and *Citizenfour* (2014, about Edward Snowden). It does not intend to condemn or endorse the leaking of classified information.

Governments around the world conduct intelligence operations to "steal secrets" of other countries, and all states classify things they don't want others to know, whether the audience is foreign or their own domestic publics. The reason most often given for withholding some information as secret or classified is for national security, but inevitably this justification gets abused, either concealing things that are highly embarrassing but not a security threat or things which are clearly in the public interest despite whatever threat they may pose. Note that saying something is classified is stronger than calling it sensitive 敏感的; a better but still not equivalent translation might be 内部的. Certainly, every state government finds different kinds of information worth putting under classification and has different rules for gaining access to it.

Advocates of radical transparency, often anarchists, hackers 黑客, Libertarians, and technology utopians, reject all forms of state secrecy on grounds of public interest, free information, and free speech. Their active agenda seeks to obtain and then leak classified documents and information to the public, often by first revealing it to mass media. As liberal democracies fully expect their media to conduct investigative reporting and serve as outlets for government transparency, media exposés lend the whisteblowers or original leakers both a large audience and some sense of legitimacy. Governments themselves rarely use the term "whistleblower," instead treating the individuals, groups, and media outlets responsible for leaks as criminally liable, often under the Espionage Act of 1917.

Organizations like Transparency International (www.transparency.org), in contrast with both extreme secrecy and radical transparency, favor a more moderate standard of open governance similar to that of most Western, liberal democracies, not least because openness helps to keep the public (and voters) informed about what the government is doing. Under the Freedom of Information Act 信息自由法令 in the USA, the government must provide non-classified documents to citizens upon their request. Furthermore, classifications expire after ten years unless renewed, and declassified documents from decades past often offer opportunities to revise history. Increasingly, the salaries of public employees including government workers and public university professors are made freely available as a means to prevent corruption, though many such workers likely feel this is an invasion of personal privacy.

Levels of document classification in the U.S. start by default as non-classified, meaning they can be accessed and distributed without a security clearance. From there, the possible damage to national security from public disclosure determines the level of secrecy required. The lowest level of classified documents are confidential, mid-level are secret, and the highest are top secret 绝密的 (to which only about 1.4 million Americans are authorized to read). Since 9-11, U.S. officials describe the expansion of the number of individuals authorized to read classified documents as a philosophical shift from a restrictive "need-to-know" to an expansive "need-to-share" (between government departments and among allies) to prevent future terrorist attacks.

Discussion questions: To what extent is control of information necessary for national security? Are whisteblowers criminals or heroes? Under what circumstances might you "blow the whistle" on your employer? How does the internet help and hurt governments or advocates of radical transparency (i.e. Wikileaks)?

The U.S. Intelligence Community (IC) handles decisions and information related to state secrets and has 16 member agencies subject to oversight by both the Executive and Legislative branches of government.

A list of some government/police activities which are supposed to be illegal in the U.S.: ·entering one's home without a search warrant (search & seizure) ·detainment without charging someone of a crime ·incarceration, execution, or other punishment without "due process of law" ·racial profiling (i.e. police stopping cars driven by some races more than others) ·surveillance of citizens not under suspicion for having committed a crime

Vocabulary: ·(The) ACLU (American Civil Liberties Union) ·access Sth. Vs. have access to Sth. ·access denied ·(intelligence) agent 情报员 ·(political) asylum 政治避难 ·break a code/encryption ·bug (Sb.'s phone) ·civil liberties ·classified information ·classify (Sth.) VS. de-classify (Sth.) ·code name 代号 ·(Sth. is) common knowledge ·confidant 知己 ·confidential/confidentiality ·covert ·cybercrime ·cybersecurity 网络安全 ·cyberwarfare ·damage control 损害管制 ·data mining 数据挖掘 ·data theft ·disclose Sth. (to Sb.) ·document-disclosure ·disregard (Sth./Sb.) 蔑视 ·encode/decode Sth. ·encryption ·encrypted transmission ·enemy of the state ·espionage ·expose/reveal (Sth./Sb.) ·exposé ·firestorm ·gag order ·gatekeeper ·informant 通知者 ·information security ·intercept (a message or other transmission) ·(for) internal (i.e. CCP/Party) reference 内部的 ·internal memorandum (memo) ·invasion of privacy 侵犯隐私(权) ·"lights on, rats out" ·mishandle Sth. (i.e. classified documents)不当处理 ·(to be on a) need-to-know basis (only those who "need to know" will receive or be allowed to access certain sensitive information) ·redact/black-out Sth. (i.e. sensitive names and text from a document) ·paper shredder ·paranoia 偏执狂 ·phishing (e-mail to steal passwords, credit card information, etc.)钓鱼式攻击 ·precautionary measures 预防措施 ·privileged information 特许信息 ·protect one's source (of information) (not reveal where information came from) ·(Sth. is in the) public domain ·security breach ·"shadow government" ·shed light on Sth. ·snitch (someone who reports a crime committed by an associate to the authorities)告密者 ·source (of information) ·state secret(s) ·sunshine laws ·"throw the book" (at Sb.)警告某人应按规定办 ·trace (a call/computer) back to... ·treason ·(go) undercover ·violation of trust/betrayal ·wiretapping ·(to) wear a wire/be wired ·whitewash/sanitize (Sth. embarrassing/damaging) ·whistleblower