ORCON CREEP:
NETWORKED GOVERNANCE, INFORMATION SHARING, AND THE THREAT TO
GOVERNMENT ACCOUNTABILITY

Alasdair Roberts
Director
Campbell Public Affairs Institute
The Maxwell School of Syracuse University

October 2, 2003

Abstract. Many policymakers suggest that an effective response to terrorist threats will require more extensive sharing of information among government agencies. Traditionally, governments have insisted on applying the rule of originator control -- ORCON -- before they share information with other governments. The ORCON rule allows originating governments to retain control over the declassification of information (if it is classified) or its release to non-governmental parties. The ORCON rule is being widely applied as the U.S. government responds to the terror attacks of September 11. However, the ORCON rule clashes with the principles underlying most right-to-information laws, and its extension could undermine governmental accountability. A better approach would allow for the structured decentralization of discretion about the public disclosure of shared information.
INTRODUCTION

Even before the terror attacks of September 11, it seemed clear to some policymakers that the nation's ability to preserve homeland security was being undermined by weaknesses in information sharing. In February 2001, the Hart-Rudman Commission on National Security in the 21st Century warned that "a direct attack against American citizens on American soil is likely over the next quarter century" and that the risk was aggravated by the failure to share information -- with friendly governments, about the structure and schemes of terrorist networks; among border control agencies, about the entry of dangerous persons or cargo; between government agencies and private firms, about the vulnerability of privately-operated utilities and computer systems; or between intelligence, police, fire and healthcare agencies, about imminent threats and plans for responding to emergencies (Commission on National Security/21st Century 2001).

The proposition that national vulnerabilities had been made worse by the failure to share information was affirmed after the terror attacks. "Information was not sufficiently shared," said the Congressional Joint Inquiry into September 11, in its December 2002 report. Federal agencies "did not bring together and fully appreciate a range of information that could have greatly enhanced its chances of uncovering and preventing Usama Bin Ladin's plan to attack these United States on September 11th, 2001" (Congressional Joint Inquiry 2002). The Central Intelligence Agency had not collected important information about Al Qaeda from foreign intelligence services, or shared its own intelligence with the Federal Bureau of Investigation. Regional offices of the FBI had not shared information about investigations about related terrorist threats. The CIA and FBI had both failed to warn the Immigration and Naturalization Service that newly discovered Al Qaeda associates should be added to the INS watch list. The
National Security Agency had not translated or disseminated intercepted messages that might have been relevant to the September 11 plot (Congressional Joint Inquiry 2002; Miller, Stone et al. 2002).

The problem of inadequate communication was also emphasized in the post-attack assessments of the performance of New York City's emergency services. A McKinsey & Company report found that the New York Police Department undertook "minimal intelligence sharing with federal agencies" and lacked procedures for collecting and distributing accurate information about the attacks within the department itself. Leaders of the Fire Department were also hindered by a lack of reliable information on the morning of the attacks, as well as technical difficulties that limited communication among units that had responded to the attacks. The two departments said McKinsey, "rarely exchanged information related to command and control" (McKinsey & Company 2002a, 28, 37; McKinsey & Company 2002b, 7-9). Similar troubles compromised the work of emergency services in Washington (Perlman 2003).

Governmental failures in information sharing were contrasted with the presumed strengths of Al Qaeda itself. The terrorists "worked together," said the journalist John Miller, who had tracked Al Qaeda for a decade, "That was one of the terrorists' great strengths. . . They shared critical tactical information across units" (Miller, Stone et al. 2002, : 296). Al Qaeda seemed to be structured as an "all channel" or "full matrix" network, in which each cell was able to communicate easily with all others. "All channel data flow" made Al Qaeda more agile and resilient to attack. To fight the terrorists, government agencies would have to learn from their structure. It would be necessary, John Arquilla and David Ronfeldt of RAND, to "fight networks with networks." Sharing information with partners in the terror-fighting network would have to become the norm (Arquilla and Ronfeldt 2001a; Arquilla and Ronfeldt 2001b).
Within a year, the need for improved communication between agencies became one of the orthodoxies of reform within the federal government. In July 2002, the Office of Homeland Security listed information sharing as one of the "four foundations" of homeland security (Office of Homeland Security 2002, x). The Office proposed to build

... a national environment that enables the sharing of essential homeland security information. We must build a 'system of systems' that can provide the right information to the right people at all times. Information will be shared 'horizontally' across each level of government and 'vertically' among federal, state, and local governments, private industry, and citizens. With the proper use of people, processes, and technology, homeland security officials throughout the United States can have complete and common awareness of threats and vulnerabilities as well as knowledge of the personnel and resources available to address these threats. Officials will receive the information they need so they can anticipate threats and respond rapidly and effectively (Office of Homeland Security 2002, 56).

"Sharing information," Homeland Security Tom Ridge told governors in August 2003, "is at the heart of what we do as a country" (Janofsky 2003).

There are many barriers that must be overcome to improve the sharing of information within new terror-fighting networks -- and some barriers that should not be overcome. Fourth Amendment protections against unreasonable search and seizure limit the ability of agencies engaged in counterintelligence efforts to share information with agencies concerned with the prosecution of criminal offences. The Defense Advanced Research Projects Agency identified over two dozen federal laws, including the Privacy Act, that were expected to constrain the
development of its Terrorist Information Awareness project, which it said would allow data sharing and collaborative problem solving "across agency boundaries" (DARPA 2003, 22). In addition there are technical obstacles, such as lack of compatibility and interoperability among agencies' communications and information technology systems. Finally, there are bureaucratic and cultural constraints: histories of distrust between organizations; a lack of informal ties connecting personnel in different agencies; or concern on the part of one agency that its projects will be jeopardized if information is shared with another.

Agencies that are asked to share sensitive information may also fear that it will be released or diverted to individuals or organizations that will use it to harm the public interest. As a consequence, agencies will seek assurances from their partners that their information will be handled carefully. Agencies within a network will be expected to comply with norms or rules designed to ensure the security of shared information.

One of the most commonly applied rules of information security is known as *originator control*. Under the rule, the agency that provides information (call it Agency A) retains complete control over its dissemination by the agency which receives it (Agency B). If the information has been classified by Agency A, it cannot be reclassified or declassified by Agency B, unless Agency A consents to the change. Similarly, no information provided by Agency A can be given by Agency B to a third party -- such as another government, non-governmental organization or citizen -- without the consent of Agency A. Agency A’s control over shared information is absolute. There are no norms or review mechanisms that compel Agency A to justify its
decision to refuse a request for declassification or release of information which it has provided to Agency B. The rule of originator control is also known by its acronym, ORCON.¹

As American governments have responded to the terror attacks of September 11, the influence of the ORCON rule has expanded. While this may encourage information sharing, it also creates another difficulty: the erosion of governmental transparency. ORCON conflicts directly with the principle -- expressed through national, state and local open government laws -- that information should be publicly accessible if, on balance, the public interest is better served by its release. The ORCON rule eliminates the ability of agencies to make judgments about the wisdom of releasing shared information.

Observers have already suggested that the expansion of "networked" forms of governance could lead to a weakening of governmental accountability -- primarily through the blurring of individual agencies' responsibility for jointly taken actions. The expansion of the ORCON rule, and the weakening of transparency rules, could also corrode governmental accountability. This is not an inevitable outcome of closer collaboration. The threat to transparency would be reduced if agencies agreed on information security rules that decentralize authority to make judgments about the wisdom of releasing shared information.

ORIGINS OF ORCON

The concept of originator control is old and well entrenched in the fields of international relations and national defense, even though it may not be recognized by that name. In

¹ The acronym -- or a shorter version, OC -- is used as a document marking by U.S. military and intelligence agencies, to indicate that dissemination or extraction of information contained in the document is controlled by its originator. In the last decade, the acronym has also been used in the field of information technology, to describe an approach to control of digitized information in the public and private sectors.
diplomacy, it is recognized as a norm of intergovernmental relations, and in national defense, it is codified within classification systems established for the management of sensitive information. Open government laws such as the U.S. Freedom of Information Act, adopted after the consolidation of ORCON in these fields, have been drafted to accommodate the ORCON rule.

*Diplomacy and ORCON.* International diplomacy is one of the oldest forms of "networked governance" -- an attempt by autonomous states to manage conflicts or coordinate activities through discourse. Information sharing is integral to diplomacy: in fact, G.R. Berridge defines diplomacy "as communication between officials designed to promote foreign policy either by formal agreement or tacit adjustment" (Berridge 2002, 107 1). Over time diplomats have also developed rules about the treatment of information exchanged with other states. The rule is not formalized; rather, it is a convention or norm that has emerged over centuries.

The norm is straightforward. It is presumed that information exchanged through diplomatic channels is provided in confidence, and cannot be released without the consent of the government that provided it. The norm is justified as a practical necessity, which reflects the difficulty of managing intergovernmental relations with a high degree of transparency and the severe costs to states if relations are not managed well (Rosoux 2003). To a degree, the norm is also an anachronism, a product of a time when elites expected to govern without active popular influence. This premise may be increasingly untenable, but the norm continues to hold influence in foreign ministries. "There is an established background expectation of confidentiality for diplomatic communications, the breach of which would damage the United States' foreign relations," the Clinton administration argued in 1999 (US DOJ 1999).

It is this norm of confidentiality that has frustrated popular demands for improved transparency in intergovernmental organizations. The World Trade Organization, World Bank
and International Monetary Fund have been pressured for several years to improve public access to documents received from member states, but have refused to adopt policies that would allow their secretariats to release information without the consent of the government that provided it. Information is regarded as property of the state even after it is shared. These organizations have preferred instead to use moral suasion in effort to induce governments to accede to a presumption that they consent to the release of shared information (Roberts Forthcoming).

The intergovernmental organization with the most highly evolved policy on public access to information is probably the European Union. However, even this policy has been drafted to accommodate the ORCON rule. The first EU policy, adopted in 1993, denied any right of public access to documents provided to EU institutions by member states. Requests for such documents were referred to the governments that provided the documents. This so-called "authorship rule" was essentially a restatement of the ORCON principle. The principle was continued in a new EU policy adopted in 2000, which gives member states the right to veto the disclosure of shared information.

National security and ORCON. The ORCON rule is also deeply entrenched in the more bureaucratic system of information sharing and control developed in the U.S. national security establishment in the early years of the Cold War. The basic rules for this system are now contained in Executive Order 12958. Executive Order 12958 sets a common set of rules for the protection of sensitive information, and thereby encourages the sharing of information within and among federal agencies. The rules apply only to information that has been "classified" at one of three levels of sensitivity -- Confidential, Secret, and Top Secret.

\[\footnote{This executive order was issued by the Clinton administration in 1995. It was amended by the Bush administration in Executive Order 13292, issued in March 2003. These amendments are described later in the paper.}\]
ORCON provides the bedrock of the classification system. Executive Order 12958 says that "classified information shall remain under the control of the originating agency" even when it passes into the hands of another agency within the executive branch.\textsuperscript{3} Classified information cannot be declassified or disclosed without the authorization of the originating agency. Personnel who have clearance to view classified information must also sign nondisclosure agreements that emphasize the penalties for unauthorized disclosure. If information passes outside the executive branch -- to another branch of government, or to government contractors -- steps must be taken to ensure that ORCON rules continue to apply.

The United States' principal allies have adopted similar policies for the control of "classified" information. In fact, many allies felt pressure to adopt comparable policies as a prerequisite to the negotiation of agreements on the exchange of sensitive information with the United States.\textsuperscript{4} These agreements continue the ORCON rule: for example, the U.S. government is required to maintain the classification of information received from an allied government, and is prohibited from declassifying or disclosing such information without the allied government's approval.\textsuperscript{5}

(The importance of these bilateral commitments was recently illustrated during the controversy over the accuracy of British and American claims that the Iraqi government had attempted to procure uranium from Niger. While American policymakers conceded that their claim was not well-substantiated, British policymakers continued to insist on the reasonableness

\textsuperscript{3} §4(1)(c).
\textsuperscript{4} National Security Decision Memorandum 119, signed by President Nixon in July 1971, confirmed this practice, which had been followed by the U.S. government since the end of the Second World War.
of the claim, arguing that it was based on intelligence received from foreign intelligence services that had not been shared with its main ally. This intelligence was not shared, with the United States, a British official explained, because it "was not ours to share" (Adams and Huband 2003).

ORCON and right-to-information laws. The ORCON rule is designed to ensure that control over information remains centralized even when the information itself is diffused through a network of agencies. By contrast, right-to-information (RTI) laws such as the United States' Freedom of Information Act, which give citizens a right of access to documents held by government agencies, are built on a contrary principle. As a general rule, agencies are assumed to have discretion over the disclosure of release of information that is under their control, and expected to exercise that discretion based on a weighing of the potential benefits and harms resulting from disclosure. Even if information is transmitted to an agency by another individual or business, discretion remains with the agency, although the other party's interests may need to be considered. However, most national RTI laws were adopted well after diplomatic norms of confidentiality and classification systems had become entrenched. As a consequence the tendency has been to draft new RTI laws to fit the older practices.

For example, the United States' Freedom of Information Act (FOIA) does not acknowledge a right of access to information that has been properly classified. Courts could intervene to make judgments about the reasonableness of classification decisions, but have

---


6 5 United States Code §552(b)(1).
proved reluctant to do this.\textsuperscript{7} Intergovernmental agreements oblige the U.S. government to maintain the classification of information received from foreign governments, and as a consequence this information is also protected from disclosure under FOIA. Unclassified information received from foreign governments can also be classified by U.S. agencies, on the grounds that the act of disclosure without consent would undermine international relations and thus harm to national security (US DOJ 2002, 108 and 112-113). This position is buttressed as a result of recent Bush administration amendments to Executive Order 12958, which now says that the unauthorized disclosure of foreign government information is \textit{presumed} to harm national security, in which case classification is justified.\textsuperscript{8} In sum, the FOIA has been drafted and interpreted to ensure that the ORCON principle will not be violated, either with regard to the norm of diplomatic confidentiality or the classification system.

Many of the United States' key allies\textsuperscript{9} have also crafted their RTI policies to protect the ORCON principle, particularly with regard to the handling of foreign government information. The United Kingdom's code on access to information does not apply to information received in confidence from other governments, "whether or not harm would be caused by the release of the particular information in question" (United Kingdom 1997, 26). (The UK's new Freedom of Information Act, scheduled to come into force in 2005, will provide similar protection.) Australia's Freedom of Information Act also exempts information received in confidence from other governments, and allows the government to issue a "conclusive certificate" that blocks any

\textsuperscript{7} For a recent statement of this position, see \textit{Center for National Security Studies v. United States Department of Justice}, 331 F.3d 918 (D.C. Cir. 2003).

\textsuperscript{8} § 1.1(c).

\textsuperscript{9} The group of countries sometimes known by the acronym AUSCANNZUKUS -- Australia, Canada, New Zealand, and the United Kingdom, as well as the United States itself.
appeal against the decision to deny access to such information. Canada's Access to Information Act takes the same position. New Zealand law says that broader public interest considerations need not be taken into account in decisions to withhold information received in confidence from other governments. In all of these cases the right to information has been subordinated to accommodate the principle of originator control.

HOMELAND SECURITY AND ORCON CREEP

The new emphasis on homeland security, and on the importance of building "all-channel networks" among government agencies to fight terrorist threats, has resulted in the extension of the ORCON rule in the domestic sphere. "All-channel networks" require deep information sharing, and information sharing in turn requires clear rules about the terms on which information will be shared. One common response has been to adopt ORCON as one of these ground rules. This is most obvious with regard to the extension of the classification system following the September 11 attacks. However, ORCON is also incorporated in several other new information sharing policies that have been designed since the terror attacks. These include new rules on the sharing of sensitive but unclassified information (SBUI), Critical Infrastructure Information (CII), and Critical Energy Infrastructure Information (CEII), as well as Joint Terrorism Task Forces (JTTFs) recently established by federal law enforcement and intelligence agencies.

10 Section 33 of the Commonwealth Freedom of Information Act.

11 Section 13 of the Access to Information Act exempts information received in confidence from other governments. Section 69.1, added shortly after the September 11 attacks, gives government the power to issue certificates that eliminate the possibility of appeal.

12 Section 6 of the Official Information Act.
Sharing classified information. One symptom of ORCON creep has been the expansion of the classification system following the September 11 attacks. The classification system is a highly formalized, well-established system for protecting and sharing information, which is now being broadened to accommodate new purposes and include a broader range of officials. "By comparison to previous years," says Harold Relyea, commenting on recent trends in classification activity,

more information is classified; more of it is connected with homeland security;
[and] more of it is needed at sub national levels, because of their heightened priority and increased efforts in the field (Kaiser 2003, 216)

The broadening of the classification system also implies an extension of the ORCON protections that are integral to the system.

The adaptation of the classification system has involved, first, an extension of the range of information that is thought to require protection in the name of national security. In March 2002, White House Chief of Staff Andrew Card Jr. advised federal departments and agencies to consider classifying information that "could be reasonably be expected to assist in the development or use of weapons of mass destruction," or reclassifying information of this type that had been declassified but never disclosed to the public (Card Jr. 2002). As critics suggested, this could include information about basic or applied research supported by federal agencies that could be used for both peaceful and destructive purposes.

The Card memo urged closer consideration of authority already available under existing law. In March 2003, this was followed by an actual broadening of the criteria for classifying information. Executive Order 12958, which governs the classification system, was amended to incorporate the protection of "homeland security" as an explicit goal. (A Clinton-era
commitment to "emphasize our commitment to open government" in the post-Cold War era was also deleted.) The "national security" considerations that justify classification now include "defense against transnational terrorism." For the first time, the order also anticipates the classification of information about "infrastructures" and "protection services" for homeland security reasons.\textsuperscript{13}

The adaptation of the classification system has also involved an expansion of the range of officials authorized to classify information. Classification authority has traditionally been limited to departments and agencies directly involved in national security matters.\textsuperscript{14} In December 2001, the Bush administration gave the Department of Health and Human Services a limited authority to classify information. In May 2002, the Environmental Protection Agency received the same authority. So did the Department of Agriculture in September 2002. The Department of Homeland Security acquired more extensive classification authority shortly after its establishment in January 2003. In September 2003, the White House's Office of Science and Technology Policy also obtained more extensive classification authority.\textsuperscript{15}

\textsuperscript{13} See the preamble, §1.1(a)(4), and §§1.4(e)-(g) of Executive Order 12958, as amended by Executive Order 13292. The amendments took effect on September 22, 2003.

\textsuperscript{14} Before September 11, five of the fourteen cabinet departments had TOP SECRET classification authority (State, Treasury, Defense, Justice, and Energy); two had SECRET authority (Commerce and Transportation); and six had none (Interior, Agriculture, Labor, Health and Human Services, Housing and Urban Development, and Education.) Three departments -- Defense, State, and Justice -- accounted for well over ninety percent of all original classification decisions.

\textsuperscript{15} DHHS, DOA and EPA received SECRET authority; DHS received TOP SECRET authority. OSTP saw its authority increased from SECRET to TOP SECRET. See the Federal Register 66.239 (December 12, 2001), pages 64345-64347; Federal Register 67.189 (September 30, 2002), pages 61463-61465; Federal Register 67.90 (May 9, 2002), page 31109; and Federal Register 68.17 (January 27, 2003), pages 4072-4074. The EPA briefly held similar authority in the 1980s.
Third, the adaptation of the classification system has involved an expansion in the number and type of officials authorized to receive classified information. In particular, a large number of senior state and local officials are being incorporated into the federal classification system. Before September 11, state and local officials were unlikely to hold the security clearances required to receive classified information. "Their need for classified information," says Frederick Kaiser, had been "narrow and circumscribed -- confined, for instance, to nuclear weapons facilities or certain defense establishments within their jurisdictions" (Kaiser 2003, 215). However, there have been frequent calls to provide clearances more liberally, so that state and local officials can receive classified information about homeland security threats. The Homeland Security Act adopted in November 2002 also endorsed the granting of clearances to state and local officials to promote information sharing.16 In August 2003, Homeland Security Secretary Tom Ridge said that all state governors had received top-secret clearances that would enable them to view classified information about security threats, including information used to make decisions about changes in the federal government's color-coded terror alert. Five other officials in each state were to receive clearances for the same purpose (Janofsky 2003)

The extension of the classification system to accommodate new purposes -- the protection and sharing of homeland security information -- also implies an extension of the ORCON rules that are embedded in the classification system. For example, state and local officials will be prohibited from declassifying or disclosing classified information without the approval of the agency that classified the information. This prohibition is affirmed in the nondisclosure

---

16 Homeland Security Act, §891(b)(6).
agreement that state and local officials must sign as part of the security clearance process.\footnote{\textsuperscript{17} Homeland Security Secretary Tom Ridge recently confirmed that all state governors have signed nondisclosure agreements (Ridge 2003).} The standard agreement requires officials to promise that they will never disclose information without authorization from the classifying agency, and reminds officials of the criminal and civil penalties for unauthorized disclosure. The agreement asserts that shared classified information remains the property of the federal government, and must be returned to the federal government on its request (ISOO 2003).

These agreements will likely eliminate any possibility that information could be released in response to a request under state right-to-information laws. A state official might be able to argue that the shared information is not under the control of a state agency, and therefore not subject to state law, because of terms included in the nondisclosure argument. State laws also contain limitations on access -- such as a restriction on access to information that could, if disclosed, jeopardize public safety, or reveal criminal investigative techniques -- that could be invoked to justify the withholding of shared information.\footnote{\textsuperscript{18} As we shall note later, many laws also exempt records that are exempted by disclosure by federal statute. (For example, see New York's Public Officers Law, Art. 6, §87(2)(a).) However, the federal classification system is not based directly on statutory authority -- although there are criminal penalties for disclosure of classified information in some limited circumstances.}

If neither of these defenses is available, there could be a conflict between federal government requirements and state law. In such a case, federal restrictions seem likely to trump state access requirements. The federal government asserts that rules governing the classification system -- contained in Executive Order 12958 -- are drafted on the basis of the President's
constitutional authority to regulate information relating to national security.\textsuperscript{19} Courts are likely to accept the argument that these federal rules preempt state law, particularly if national security is said to be at risk.\textsuperscript{20}

*Sensitive Homeland Security Information (SHSI).* The concern for improved information sharing has also led to the development of new systems to govern the handling of sensitive but *unclassified* information (SBUI). In some respects, the protocols being developed for SBUI are less demanding than for classified information -- except for an equally heavy emphasis on the ORCON rule.

The category of SBU information is not well defined. Broadly, it can be characterized as information that does not qualify for classification, but which is also -- in the eyes of agency officials -- protected from disclosure through the Freedom of Information Act. There is no standard policy that prescribes the steps that must be taken to protect SBUI in federal agencies. Many agencies have developed their own directives on the handling of such information; in fact, they may call SBU information by a variety of other names -- "For Official Use Only," "Limited Use," "Limited Official Use," "Administratively Controlled," or simply "Sensitive."\textsuperscript{21}

Current rules about the dissemination of SBUI also vary, but are generally not as rigorous as for classified information. For example, Defense Department policy permits the circulation of "For Official Use Only" information to the legislative branch, other agencies, contractors, consultants, and grantees as necessary in the conduct of official business, without the need for a

\textsuperscript{19} For a recent assertion of the President's constitutional authority to regulate the flow of classified information, see his statement on the signing of the Homeland Security Act (Bush 2002.)

\textsuperscript{20} For a comparable case in which federal rules were found to preempt a state disclosure law, see: *American Civil Liberties Union of New Jersey and Jacobs v. County of Hudson et al*, 352 N.J. Super. 44, 799 A.2d 629.
non-disclosure agreement or other commitment on the handling of shared information (Department of Defense 1997, §AP3.2.3). State Department policy says that employees "may circulate SBU material to others, including Foreign Service nationals, to carry out an official U.S. Government function if not otherwise prohibited by law, regulation, or interagency agreement," and imposes no obligation to provide warnings against further distribution or negotiate nondisclosure agreements (State Department 1999, §12.543). Federal Aviation Administration rules provide for the distribution of certain types of "administratively controlled" information to airports and air carriers; while recipients are warned not to retransmit information without FAA permission, a nondisclosure agreement is not required (14 CFR 191).

The Bush administration gave new emphasis to the handling of SBUI in the months following the September 11 attacks. In October 2001, the Department of Justice advised departments that they should adopt a more restrictive interpretation of FOIA, which would reduce the risk that SBUI would be disclosed under that law.\(^2\) In March 2002, White House Chief of Staff Andrew Card Jr. urged federal departments and agencies to take "necessary and appropriate actions to safeguard sensitive but unclassified information related to America's homeland security," including compliance with the restrictive approach to the FOIA endorsed by the Justice Department a five months earlier (Card Jr. 2002).

These steps had the effect of broadening the domain of SBU information, and were principally aimed at preventing disclosure from the agencies that had produced the information.

\(^2\) A broad survey of agency practices regarding SBUI is provided by (Knezo 2003).

\(^2\) In 1993, the Attorney General Janet Reno told federal agencies that the Justice Department would defend agencies that were sued for non-disclosure only when it was "reasonably foreseeable that disclosure would be harmful" to an interest protected by the law. By contrast, Attorney General John Ashcroft told agencies that "the Department of Justice will defend your decisions unless they lack a sound legal basis" (Ashcroft 2001).
However, the Bush administration also promoted a rationalization of departmental SBUI policies, aimed not just at protection against disclosure, but also at improving the flow of SBUI among federal agencies, and with state and local governments. In doing this, the Bush administration endorsed the adoption of much stronger protections against the public disclosure of shared information. In June 2002, the White House announced its support for HR 4598, the proposed Homeland Security Information Sharing Act, which it said would "balance and reconcile the needs of State and local personnel to have access to timely and relevant homeland security information to combat terrorism with the need to protect and safeguard both classified and sensitive but unclassified information" (Office of Management and Budget 2002).

HR 4598 authorized the President to develop procedures to govern the sharing of SBU homeland security information that would apply to all federal agencies. The bill was premised on the principle of "federal control of information," stipulating that "information obtained by a State or local government from a Federal agency [under these procedures] shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such information." For added protection, the bill anticipated that state and local officials might be required to sign nondisclosure agreements before receiving SBU information.\(^{23}\)

These provisions, which firmly entrenched the ORCON rule, were combined into the Homeland Security Act (HSA) adopted in November 2002.\(^{24}\) In July 2003, responsibility for drafting the new sensitive homeland security information (SHSI) procedures was assigned to the

---

\(^{23}\) See Sections 3(c)(2)(B) and 3(e) of the Homeland Security Information Sharing Act, HR 4598, 107th Cong., 2d Sess.
Secretary of Homeland Security. There is no deadline for the implementation of the new rules, although the HSA does require the President to make a status report on progress by November 2003. There is concern that there will not be adequate opportunity for public comment on the proposed rules, and also about the likely impact of provisions designed to protect the ORCON principle. In August 2003 the advocacy group OMBWatch said:

Individuals both inside and outside of government without clearance to view classified materials would be asked to sign nondisclosure agreements and would be subject to criminal and civil penalties. According to a recent analysis, over four million people could be subject to these confidentiality agreements. Information that may be critical to business, state and local government, health officials and others may now be deemed "sensitive but unclassified" (SBU) and subject to restrictions on its disclosure to the public. DHS could use this provision to transfer previously unclassified information into this category, restricting both what and with whom people can share information. Consequently, a host of people unrelated to terrorism or its prevention, from researchers and scientists to community and trade groups, could see information access prevented or severely restricted (OMBWatch 2003).

There is certainly little doubt that the SHSI provisions contained in the HSA will be effective in blocking access through state or local records laws, most of which do not apply to records that are exempted from disclosure by federal law.


25 The assignment of responsibility was effected by Executive Order 13311, July 29, 2003.
Critical Infrastructure Information (CII). The September 11 attacks also speeded the development of new rules on the sharing of information about "critical infrastructure" -- the name given to systems or assets whose performance is considered essential to national security, economic security, or public health and safety.27 Because many of these systems and assets are privately owned, and because the burden of protecting assets and emergency response is shared with state and local governments, rules to promote more extensive sharing of "critical infrastructure information" (CII) seemed essential. These new rules also incorporate the ORCON principle.

The need to improve CII sharing had been recognized several years before the 2001 attacks. In its 1997 report, the President's Commission on Critical Infrastructure Protection argued that the evolution of information and communications technologies had increased the nation's vulnerability to attacks on infrastructure, and claimed that better information sharing was "the most immediate need" in a plan to thwart attacks. The risk of "cyber terrorism" seemed especially acute, and the report warned of "insufficient interagency, federal-to-state and local government, or public/private correlation of data to support crisis action planning in response to a cyber terrorist incident" (PCCIP 1997, 21 and 29).28

In the eyes of Commission, an important barrier to the sharing of privately held CII was the infrastructure owners' fear that shared information would become public -- resulting in

---

20 Section 893(a) of the Homeland Security Act.

27 In the USA Patriot Act adopted in October 2001, "critical infrastructure" is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (Section 1016).
damage to reputation, weakened competitive position, higher risk of legal liability, and increased pressure for government regulation. "Potential participants in an information sharing mechanism may require assurances that their sensitive information will remain confidential if shared with the federal government," the Commission concluded. It recommended that legislation to improve infrastructure security should contain a provision that excluded shared CII from disclosure requirements contained in the federal Freedom of Information Act (PCCIP 1997, 28 and 31).

The Critical Infrastructure Information Security Act of 2001, a bill introduced two weeks after the September 11 attacks, would have implemented this recommendation.  

Critics argued that the bill was too broadly drafted and unnecessary, given limits on disclosure already contained in the FOIA (Richtel 2003). However, the new preoccupation with homeland security meant that such concerns were given lesser weight. (In May 2002, Senator Bob Bennett -- one of the bill's sponsors -- added another reason for excluding CII from FOIA: such information "could be used as a road map for future terrorist attacks" (Joint Economic Committee 2002, 6).) A comparable exclusion for CII received by the new Department of Homeland Security was contained in the Homeland Security Act adopted in November 2002. Under the new law, federal officials cannot disclose shared CII for purposes other than infrastructure protection without the written consent of the organization that provided the information.

In fact, the Homeland Security Act eliminated a significant loophole in the 2001 bill. While the 2001 bill anticipated that state or local governments might receive CII provided to

---


29 S. 1456, 107th Cong., 1st Sess., Section 5.
federal agencies, it did not anticipate that such information might be still at risk of disclosure under state and local public records laws. Nor were state and local officials subject to the criminal penalty for unauthorized disclosure that would have been imposed on federal officials. By contrast, the Homeland Security Act explicitly preempts state and local public records laws, and prohibits the disclosure of CII by state and local officials without the written consent of the organization that provided the information.31

Proposed regulations to implement these provisions were published by the Department of Homeland Security in April 2003. State and local governments will be required to enter into express agreements with DHS that confirm their understanding of restrictions on disclosure of shared CII (Department of Homeland Security 2003b, Section 29.8). The regulations would require state and local governments to seek permission from the department's CII Program Manager before any proposed disclosure of CII. The Program Manager in turn will seek written consent from the organization that provided the information. The regulations also appear to adopt a broad interpretation of the law: organizations providing information to any other agency can request that it also be forwarded to DHS, thus bringing it under the protection of the Homeland Security Act's rules (Department of Homeland Security 2003b, Section 29.5).32

**Critical Energy Infrastructure Information (CEII).** The ORCON principle has also been applied to protect the flow of a specific type of CII known as critical energy infrastructure

---

30 Pub. L. No. 107-296, Section 214(a)(1)(A). This part of the Homeland Security Act is also known as the Critical Infrastructure Information Act (CIIA). An analysis of the CIIA's weaknesses is provided by (Steinzor 2003).


32 In March 2003, a group of Democratic senators introduced the Restoration of Freedom of Information Act of 2003 (S. 609, 108th Cong. 1st Sess.), which they said would relieve some of the restrictions on disclosure of CII imposed in the HSA. However, the bill did not propose to eliminate the override of state and public records laws for CII received from DHS.
information (CEII). The principle is contained in rules recently issued by the Federal Energy Regulatory Commission (FERC), the federal agency that regulates the interstate transmission of natural gas, oil, and electricity, as well as natural gas and hydropower projects.

Shortly after the September 11 attacks, FERC began to restrict access to tens of thousands of documents provided by regulated companies that had been made publicly accessible on the FERC website or in its Public Reference Room (FERC 2003, 9858). The regulator feared that the documents might reveal details about energy projects, power lines and pipelines that could be used to plan further terror attacks.

Although FERC no longer took the initiative to make this information publicly accessible, the possibility of obtaining it through a Freedom of Information Act (FOIA) request remained. (In fact, FERC received over two hundred such requests over the following year (FERC 2003, 9858).) From FERC's point of view, the FOIA system was an imperfect method of controlling access to CEII. Under FOIA, an agency has no right to consider an individual's reasons for requesting information; neither can it impose restrictions on the use or further distribution of information. Furthermore a decision to release information to one individual would prevent FERC from denying access to any other individual making the same request. In January 2002, FERC suggested that it could adopt new interpretations of FOIA rules that would allow it to block access to CEII (FERC 2002b).

33 The rule adopted by FERC in February 2003 defines CEII as "information about proposed or existing critical infrastructure that: (i) Relates to the production, generation, transportation, transmission, or distribution of energy; (ii) Could be useful to a person in planning an attack on critical infrastructure; (iii) Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552; and (iv) Does not simply give the location of the critical infrastructure." Critical infrastructure is defined as "existing and proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health or safety, or any combination of those matters" (FERC 2003).
However, there were other potential challenges to the control of CEII. A substantial amount of information collected by FERC is passed to state public utility commissions, where it becomes "the raw material from which state public utility commissions conduct day-to-day analysis, inquiries, and proceedings" (FERC 2002a). FERC has statutory authority to transmit information to state commissions without compromising its ability to withhold information from the general public under FOIA. However, state commissions must comply with state public records laws, which might create a right of access to CEII received from FERC. "A primary concern" in drafting new CEII rules, FERC said, "is the ability of state agencies, which likely will be subject to their own FOIA rules, to protect CEII received from the Commission" (FERC 2003, Para. 50).

FERC’s new CEII rules were adopted in February 2003 (FERC 2001). The Commission affirmed its intention to adopt a broad reading of provisions in FOIA that would allow it to deny access to CEII under that law. A separate procedure is established for making CEII requests, in which requesters must submit information about their identity and need for the requested information. Requesters will also be obliged to sign non-disclosure agreements (NDAs) to prevent the relay of CEII to other parties.34

New constraints are also imposed on state commissions. FERC says that it has "no intention of asking a state agency to ignore state law" (FERC 2003, Para 53). However, the objective of its policy is to reduce the possibility that CEII can be released under state law. Like other requesters, state commissions will be required to sign a non-disclosure agreement that

34 There is one exception. Owners and operators of critical energy infrastructure do not need to sign an NDA before gaining access to information regarding their own projects. FERC explained: "The reason for this is that they have at least as great an incentive to protect this information as the Commission has, and probably have access to even more damaging information in the event a rogue employee wanted to cause harm to the facility."
might create an expectation of confidentiality sufficient to block release under some state laws. NDAs will also state that CEII is provided "on loan" to state commissions and that FERC retains the right to request its return. This wording could provide state commissions with a basis for arguing that records containing CEII are not actually owned or controlled by them, and therefore not subject to state laws. As a further safeguard, FERC will also require state commissions to notify them when CEII is sought under state laws (FERC 2003, Para 57-58).

Joint Terrorism Task Forces. The terror attacks of September 2001 also prompted new attention to information sharing among federal, state and local law enforcement agencies. One of the most prominent responses to the problem of informational blockages has been the creation by the Federal Bureau of Investigation (FBI) of dozens of new Joint Terrorism Task Forces (JTTFs). However, JTTFs are carefully designed to ensure that the lead agency -- the FBI -- retains tight control over JTTF information. The controls are so stringent that it might be reasonable to ask whether JTTFs constitute a form of information sharing at all.

JTTFs are investigative teams established by field offices of the FBI, which include personnel from the FBI, other federal agencies35, and state and local law enforcement agencies. The first task force was established in New York City in 1980. In the late 1990s, federal concern about terrorist threats led to quick growth in the number of JTTFs -- from eleven in 1996 to 29 in March 2001. After September 11, all FBI field offices established a JTTF, as did ten smaller FBI offices -- a total of 66 task forces now in operation (FBI 2003).

---
35 Such as the CIA, the Bureau of Citizenship and Immigration Services, the Marshals Service, the Secret Service, the Transportation Security Administration, the Customs Service, the Bureau of Alcohol, Tobacco, and Firearms, the State Department, the U.S. Postal Inspection Service, and the IRS.
JTTFs are frequently presented as one of the federal government's most important techniques for sharing information with state and local law enforcement agencies. The head of the FBI's recently-established Information Sharing Task Force told Congress in April 2002 that JTTFs "have proven to be one of the most effective methods of unifying federal, state and local law enforcement efforts to prevent and investigate terrorist activity by ensuring that all levels of law enforcement are fully benefiting from the information possessed by each" (Jordan 2002). The Bush administration's July 2002 National Strategy for Homeland Security, and the Joint Congressional Inquiry's report on the September 11 attacks, present JTTFs as the major device for information sharing (Office of Homeland Security 2002, 25-26; Joint Inquiry 2003, 88-89 and 361). In the November 2002 Homeland Security Act, Congress also encouraged the increased use of "information sharing partnerships" such as JTTFs.36

However, the design of JTTFs actually appears to impose strict controls on the flow of information to state and local law enforcement agencies.37 Records for JTTF investigations are kept in an FBI field office, and the FBI appears to retain control over the placing of related records in the files of other agencies. State and local law enforcement personnel who are assigned to a JTTF are sworn as Special Federal Officers or Special Deputy Marshals. The act of deputation means that these state and local personnel may be regarded as federal employees for the purposes of several federal laws, including one that establishes a criminal penalty for the unauthorized disclosure of confidential information.38 The FBI may also require state and local

---

36 Section 892(c)(2)(C) of the Homeland Security Act.

37 This is a preliminary assessment based on two publicly accessible JTTF agreements currently in force: one between the FBI's Portland field office and the City of Portland; the other between the FBI's Austin field office and the University of Texas Police Department.

38 The deputation of state and local law enforcement personnel appears to be authorized by 21 USC 878. This provision stipulates that deputized personnel shall be deemed to be federal
officials assigned to a JTTF to sign nondisclosure agreements that prohibit the release of information without the approval of the FBI. In addition, law enforcement personnel face a general ethical obligation not to disclose information relating to investigations without the express consent of a commanding officer (Grant 2002), and supervisory responsibility within a JTTF typically appears to be assigned to an FBI Special Agent. Finally, JTTF agreements appear to prohibit statements to the media by any task force member without the consent of all JTTF partners.

The effectiveness of JTTFs as information sharing mechanism has been questioned because of the small number of state and local enforcement personnel who are assigned to these task forces. (In New York State, only about 250 of an estimated 69,000 police officers participate in JTTFs (Minority Staff 2003, 27).) However, the JTTF model, as a mechanism for information sharing, might be susceptible to even stronger criticism. The restrictions that are imposed on the handling of JTTF information are designed to ensure that the FBI retains tight control over the use and retransmission of information. This is an expression of the ORCON principle, and in this respect is not unique. In this case, however, the FBI appears to retain physical control of the information, and allows access only to individuals who are deemed -- through deputation -- to be FBI employees. Information may not really be shared with a state or local agency at all.

WHAT'S WRONG WITH ORCON?

---

employees for the purposes of several provisions listed in 5 USC 3374(c)(2). One of these provisions is a criminal penalty for the unauthorized disclosure of confidential information acquired in the course of an investigation (18 USC 1905).
In several ways, federal policymakers have taken steps to promote deeper flows of information among federal, state and local agencies engaged in work relating to homeland security. These new "all-channel networks" may collaborate more effectively with one another, but better information sharing comes with a substantial price tag. In every case, information-sharing policies have incorporated the ORCON rule, and strictly limited the capacity of actors within these networks to publicly disclose shared information. This will collide with public expectations about the accountability of agencies within these networks.

To illustrate the difficulty, consider this highly abstracted example. Imagine a situation in which there are ten autonomous governments, each charged with homeland security responsibilities, and each holding ten unique pieces of information about threats, vulnerabilities and countermeasures. Each government is regulated by a right-to-information (RTI) law that allows citizens in its jurisdiction to gain access to information held by that government. (For simplicity, suppose that the law allows complete access to this information.) In such a situation, governmental performance is obviously not what it could be: each government is ignorant of most of the existing and relevant information held by all governments collectively. On the other hand, accountability is good: citizens can inspect all of the information used by their own government and make judgments about the government's competence in exploiting that information.

Suppose that all governments agree to share information, and that the ORCON rule applies to all shared information. Government performance improves substantially, as the amount of information available to each government increases tenfold. But accountability becomes problematic. Citizens preserve their right of access to the ten pieces of information originally held by their own government. However, the remaining ninety pieces of information
can be released only with the consent of the originating government -- and because the originating government's discretion is complete and incontestable, it is fair to assume that consent will not be given. Citizens have only a partial view of the information used in their government's decision-making; conversely, governments can respond to criticisms by arguing that their decisions were justified based on information that they are barred -- because of ORCON -- from releasing.

(In fact, this simple abstraction outlined earlier probably understates how ORCON might affect transparency, because of two additional problems. The first is contamination -- the reluctance to release a government's own records for fear that it will incidentally reveal the content of other records protected by the ORCON rule. Contamination is increasingly likely as information sharing deepens. A government's own records may comment on, or be premised on, information provided by other governments, and it may be difficult to divulge information produced by the government itself without incidentally revealing the substance of shared information. A related problem is entanglement -- a commingling of information that is so deep that it becomes difficult to separate information that was received from a government's own sources, and information received from other governments.)

The clash of ORCON and public accountability was evident during the work of the Congressional Joint Inquiry into September 11. The Inquiry's staff complained that it was denied access to CIA information regarding its "liaison relationships" with foreign governments, while the FBI imposed strict controls on the use of foreign government information:

The FBI allowed the Joint Inquiry to review information provided by foreign governments at the FBI, but would not allow the documents or verbatim notes to be carried to the Inquiry’s offices. This limited and delayed the Inquiry’s efforts
to understand the level of cooperation displayed by the [name of government withheld] and other governments in counterterrorism efforts prior to September 11 (Joint Inquiry 2003, Appendix).

Access to information shared within the US government was also compromised by ORCON rules. Federal agencies refused to share information "until the originating agency had been consulted and given its permission" -- an approach that "slowed the disclosure process significantly" (Joint Inquiry 2003, Appendix). Senator Richard Shelby also complained that the Inquiry suffered "frequent delays" that were attributed to "the necessity of clearing ORCON transmittals to Congress" (Joint Inquiry 2003, Shelby). These restrictions were imposed even though the Inquiry staff was itself subject to nondisclosure rules while handling information provided by the intelligence community. The report of the Joint Inquiry was only publicly released after further negotiations with federal agencies that resulted in the removal of a large amount of sensitive information relating to foreign governments.

ORCON has also been criticized as an impediment to effective information sharing among government agencies. For example, it limits the capacity of a receiving agency to forward the information to third agency without consent of the originator, even if the third agency might have a real and immediate need for the information. In this context, the application of ORCON as the "default position" has been strongly criticized by the head of the Information Security Oversight Office, which oversees the federal classification system:

[O]riginators of information . . . are not omniscient and cannot be cognizant of all possible users of the information and how it can be applied. Also, today's environment highlights the fact that as strong as the originating agency's equities [that is, interests] may be, they do not automatically take precedence over all
others. Even more profound consequences may occur should information not be effectively shared (Leonard 2003)

A less restrictive approach would be to allow receiving agencies discretion to re-transmit information to third agencies, perhaps after consultation with the originating agency. In fact, a step toward this approach was taken in recent amendments to Executive Order 12958, which governs the federal classification system. The amended executive order allows federal agencies to retransmit classified information to individuals lacking security clearance "in an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland," without seeking the consent of the originating agency. However, this is a very limited exception to the ORCON rule. It is limited to classified information, may be invoked by federal agencies alone, and only in extraordinary circumstances, subject to conditions to be stipulated by the Director of Central Intelligence.39

A similar logic can be applied to decisions about the public disclosure of shared information. Originating agencies may have the best appreciation of the interests that might be adversely affected by disclosure of information. But their view of the interests at stake will not be complete. Originating agencies may be blind or indifferent to the interests -- such as improved accountability or trust in government -- that would be served by public disclosure by the receiving agency. The receiving agency is likely to have a better appreciation of these interests. However, the ORCON principle denies the receiving agency any discretion to take these interests into account. The originating agency, with its partial view, retains complete discretion.

A better approach would be one that strikes a better balance between security and accountability. This approach would decentralize discretion over the release of shared information, so that receiving governments have the ability to weigh contending interests. Decentralization does not imply a complete abandonment of rules about the handling of shared information. Information could be shared after an assurance that the disclosure law of the receiving government accounts properly for competing interests. Alternatively information could be shared contingent on an explicit understanding about the processes that will be used to make judgments about disclosure -- contained in a qualified disclosure agreement, rather than a nondisclosure agreement. Any such agreement could also include a right for originating governments to be consulted before decisions about release are made.

Roughly comparable policies are already adopted in other contexts. For example, many countries have adopted Mutual Legal Assistance Treaties (MLATs) that are designed to promote the sharing of information needed for criminal prosecutions. In these circumstances, the use of shared information often requires its disclosure, and MLATs must accommodate this reality by incorporating more liberal rules on the use of shared information. For example, the United States-United Kingdom MLAT, signed in 1994, states that the originating government may seek to impose restrictions on the use of shared information, but no such restrictions can trump disclosure obligations that are imposed on the receiving government by its national law or constitution. The originating government can refuse to share information, but the agreement anticipates that this will be done only when disclosure would jeopardize the "essential interests" of the state or "important public policy."40 The approach contained in MLATs still give

---

40 Treaty on mutual legal assistance in criminal matters between the United Kingdom and United States of America, with appendices and exchange of notes, January 6, 1994. See articles 3 and 7 of the Treaty, and paragraph (c) of the accompanying note from the United Kingdom.
substantial control to originating governments, but there is at least the beginning of an attempt to accommodate disclosure requirements that are imposed on receiving governments.

ACCOUNTABILITY IN NETWORK FORMS OF ORGANIZATION

Even before the terror attacks of September 2001, it was common to argue that the American public sector was entering a new age of "networked governance" -- an age in which public programs are executed by the joint action of actors or organizations that are not organized in a neat hierarchy, connected by clear lines of authority. At the "street level" of government, for example, a social services may be delivered to citizens by an array of largely autonomous agencies; and at the highest level, global economic and trade policies must be managed through the collaboration of sovereign states.

The growth of network forms of organization has provoked concern about the erosion of democratic accountability (O'Toole Jr. 1997; Agranoff and McGuire 2001). This concern is typically expressed in three distinct ways. First, there is fear about the erosion of oversight or control by political executives or legislators that may result when responsibilities are shifted to more autonomous agencies. Second, there are worries that the assignment of individual responsibility for poor performance may become more difficult when outputs are the joint product of many actors. Finally, there are the problems that arise when the networks span jurisdictions, and the capacity of individual network members to respond to their own electorates is compromised by the need to coordinate with the rest of the network.

These are important problems, but they do not exhaust the ways in which networked forms of organization could compromise accountability. By definition, there will be substantial
information flows among the members of any network, and there will be rules about the handling of shared information. Some of these rules maybe tacit, and others may be formalized in information-sharing policies. If these rules include the ORCON principle, an increasing amount of information held by each member of the network will be completely blocked from public access. The problems of contamination and entanglement could also mean that access to an agency's own information (that is, information never received from another government) could also be restricted. The public's capacity to understand how agencies reached decisions -- and to judge whether agency actions were well substantiated -- would be undermined.

An irony of contemporary governance is that many public agencies are confronted with two powerful pressures. On one hand, there are growing expectations about governmental transparency. This is manifested in the rapid diffusion of right to information laws (Banisar 2003), and in public pressure for immediate and open investigations into allegations of government misconduct. (The Hutton Inquiry, launched by the Blair government following the suicide of Dr. David Kelly, provides a vivid illustration of this phenomenon. The British bureaucracy is notorious for its secrecy; nevertheless, the inquiry quickly published an extraordinary amount of internal correspondence and email on the Internet.\(^\text{41}\)) On the other hand, there is also pressure on governments to improve performance by building "all-channel networks" among government agencies, and a temptation to extend ORCON rules in the process of building these networks.

These two pressures conflict with one another. One promotes greater openness, while the other promotes greater secrecy. As government networks become more extensive, the collision of principles will become more obvious. The conflict can be resolved by revised rules on

\(^{41}\) The material was made available at http://www.the-hutton-inquiry.org.uk/.
information sharing that allow the structured decentralization of discretion over public disclosure of shared information.
Sources


Arquilla, John and David Ronfeldt. 2001b. *Networks and Netwars: The Future of Terror, Crime and Militancy*. Santa Monica, California: RAND.


