An Occasional Paper

Number 23
2008

Counteracting Ambition: Applying Corporate Compliance and Ethics to the Separation of Powers Concerns with Domestic Surveillance

meet changing threats, while ensuring that flexibility is not a pretext for abuse. To begin answering this challenge, this Essay draws on expertise from an area of private law: the design, implementation, and operation of corporate compliance and ethics programs. A company's compliance and ethics program consists of the personnel, policies, and procedures that ensure employees and agents adhere to the company's legal and ethical obligations. For example, if a company has agents that do business overseas, it must address the concern that those agents might bribe foreign government officials to obtain business. The company should draft policies addressing payments to foreign government officials, train its agents on the relevant policies, monitor and audit its agents' expense statements, investigate suspicious activity, and discipline those who violate the policy.

My thesis is that constitutional separation of powers analysis

principle applies to the rulers as well as the ruled, for a "government of the people, by the people, and for the people"[18] will necessarily be "the greatest of all reflections on human nature."[19] Consequently, "[i]n framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself."[20] This is an application of Lord Acton's Dictum: "Power tends to corrupt; absolute power corrupts absolutely."[21] The question is how best to get the government to "control itself."

"Ambition must be made to counteract ambition."[22]

This quote begins to answer how government might control the rulers—a form of intra-governmental divide and conquer. Later in the same passage, Madison elaborates on his point:

a person is an unlawful enemy combatant subject to trial before a military commission.[30]

Generally speaking, arguments for judicial deference are appropriate, as the judiciary must guard against accumulating too much power within its own hands (*i.e.*, tyranny of the judiciary). The case for deference, however, is weakest when individual liberties are at stake. Claims of individual liberties often arise in cases where an

Judge Posner describes the types of searches data-mining might include:

> Because of the volume involved, massive amounts of intercepted data must first be sifted by computers. The sifting can take two forms. One is a search for

Similarly, private firms routinely analyze such data:

> To be assembled, retrieved, sorted, and sifted, so that patterns can be discerned and inferences drawn, intelligence data must be digitized, and the digitized data organized in databases linked to thousands of workstations (terminals, laptops, cellphones, in-vehicle displays, etc.) scattered throughout the intelligence system, not to mention tens of thousands of workstations elsewhere in the nation's farflung, poorly integrated, federal, state, local, and private security network. But that to (ee22.219arflungi.1 (fa) -9.9 (to) -uni)4fes5 193.50423wote

A. Compliance Generally

All businesses take some measures to ensure that their employees and agents comply with applicable laws. After all, the simple directive to "be careful" is an informal attempt to comply with the negligence duty of care. Compliance and ethics programs formalize and expand upon these ad hoc efforts. The formality comes from designating personnel responsible for the compliance and ethics program, and implementing organizational infrastructures that carry out the various compliance and ethics functions. The expansion comes from a comprehensive attempt to identify and address the organization's legal risks and ethical principles.

Historically, businesses have had two main reasons to implement a compliance and ethics program. First, such programs hold the promise of reducing misconduct by both educating employees about their legal responsibilities and deterring potential wrongdoers. Compliance and ethics programs, then, are sensible when the expected reduction in liability costs exceeds the cost of implementing the program. Second, after prosecuting an organization for wrongdoing, the government has often required implementation of a compliance and ethics program. This occurred after industry scandals involving price fixing, insider trading, and health care fraud.

Over the last fifteen years, the incentives towards compliance have themselves become more formal. The trend began in 1991 when the United States Sentencing Commission promulgated organizational sentencing guidelines that mandated leniency for organizations that had an effective compliance and ethics program.[42] Since then, a variety of state and federal agencies have encouraged compliance and ethics programs through guidance or incentives. For example, the United States Department of Justice has directed United States Attorneys to consider either deferring or declining prosecution of organizations that have an effective compliance and ethics program.[43] In addition, an effective program can defend against civil vicarious liability for sexual harassment, commodities fraud,[44] or workplace safety violations.[45] And a recent wave of laws and regulations *require* compliance and ethics programs, making the program *itself* an aspect of complying with the law. The clear legal

trend is toward greater emphasis on private compliance and ethics programs.

While compliance and ethics programs cover a variety of risks and industries, they contain a basic set of elements regardless of the organization. The following ten steps are core requirements of an effective program:

1. Periodic risk assessments

> dosage; and the name, address, and age of the patient. One copy of the form is retained by the physician, the second by the pharmacist, and the third is forwarded to the New York State Department of Health in Albany. A prescription made on an official form may not exceed a 30-day supply, and may not be refilled.[48]

The database was supposed to reduce drug misuse in two ways. First, the state could analyze the data for patterns that indicated illegal use. Second, enhanced detection would deter misuse.

Similar to the data-mining described above, the New York database accumulated immense amounts of data concerning legitimate activity (here, legal drug prescriptions) to detect the few cases of illegal activity (here, drug abuse). For example, during the first twenty months that the database operated, the state collected an average of 100,000 prescription forms a month, and the data contributed to only two drug misuse investigations. This led the plaintiffs to characterize the database as "a vast state system that uses a dragnet more likely to expose the names of patients seeking drugs for legitimate medically indicated use than those obtaining drugs for illicit purposes."[49]

The plaintiffs, who were prescribed drugs covered by the record-keeping provision, argued that the database threatened harm due to misuse or disclosure of their data. Misuse could consist of the state stereotyping an individual in the database as a drug addict and discriminating against the person on that basis. Disclosure could occur either through a state employee leaking the information or an outsider gaining unauthorized access. These fears, in turn, allegedly discouraged patients from seeking needed medications. Note that these arguments parallel those regarding modern domestic surveillance: Centralized collection of data exponentially increases the harm posed by abuse of the data.

The Supreme Court upheld the database largely due to state-mandated controls that minimized the threat of abuse:

> [P]rescription forms are delivered to a receiving room at the Department of Health in Albany each month. They are sorted, coded, and logged and then taken to another room where the data on the forms is recorded on magnetic tapes for processing by a computer. Thereafter, the forms are returned to the receiving

> room to be retained in a vault for a five-year period and then destroyed as required by the statute. The receiving room is surrounded by a locked wire fence and protected by an alarm system. The computer tapes containing the prescription data are kept in a locked cabinet. When the tapes are used, the computer is run "off-line," which means that no terminal outside of the computer room can read or record any information. Public disclosure of the identity of patients is expressly prohibited by the statute and by a Department of Health regulation. Willful violation of these prohibitions is a crime punishable by up to one year in prison and a $2,000 fine.[50]

Here, one can glimpse aspects of an effective compliance and ethics program. For example, the state had a policy prohibiting the disclosure of patient information as well as specified punishment for a violation. Further, the Court saw evidence that the controls actually worked, as there was no evidence of problems with the New York database or similar databases in two other states. One would want to know, however, whether the state had other compliance functions, such as whether there was auditing or monitoring for violations of this non-disclosure rule.

The Court concluded its opinion by leaving open the question what role the existence of data security measures should play in future analysis:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative proce-

> dures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data whether intentional or unintentional *or by a system that did not contain comparable security provisions*. We simply hold that this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment.[51]

This passage yields two points relevant to the current analysis. First, in reviewing the constitutionality of government collection, analysis, and storage of citizen data, a court should consider what safeguards the government has implemented to prevent improper use or disclosure of the data. These safeguards are in essence compliance and ethics measures tailored to data security. Second, since *Whalen* was decided in 1977, the understanding and requirements of an effective compliance and ethics program in general, and for data security specifically, have changed dramatically. The next Part suggests that *Whalen*'s insight about the constitutional relevance of compliance measures be updated to take account of the increased formality and sophistication of modern compliance and ethics programs.

IV. Putting It All Together: A Separation of Powers Proposal

The preceding sections of this paper discuss aspects of the separation of powers, constitutional protections for private information, and compliance and ethic programs. The following

branches—the President and Congress—may not be adequately motivated to protect individual liberties, as when the claimed liberty is unpopular.

Third, modern domestic surveillance, even in aid of foreign intelligence, entails the collection and storage of massive amounts of private data concerning United States citizens. Citizens rightly fear that such data could be either misused or improperly disclosed, raising issues of individual liberty that (at times) may be unpopular. Separation of powers suggests that the federal judiciary ought to be

as whether the corporate compliance officer ought to report through the organization's legal department or directly to the CEO or a board committee. But courts can apply the consensus standards and give deference where consensus runs out.

Second, we know that evaluating compliance and ethics

and balances—is the first line of defense against such incursions. Our timeless commitment to separated power must now be applied to the

Endnotes

1 This essay extends my remarks delivered at the conference "Guarding the Guardians: The Ethics and Law of Domestic Surveillance," hosted by the Cary M. Maguire Center for Ethics and Professional Responsibility at Southern Methodist University on October 20, 2006. I thank my co-presenters for their comments and questions on my presentation. Also, special thanks to

13 After I had presented this paper, the Department of Justice announced that it was implementing additional internal controls over its national security activities. See Letter from Alberto Gonzales to Richard B. Cheney, dated July

39 Richard A. Posner, *Uncertain Shield: The U.S. Intelligence System in the Throes of Reform* (Rowman & Littlefield Publishers, 2006), 141 .
40 Ibid., 141-42.
41 429 U.S. 589 (1976).
42 Amendments to the Sentencing Guidelines for United States Courts, 56 Fed. Reg. 22,762 (May 16, 1991).
43 Memorandum from Paul J. McNulty, Deputy Attorney General, to Heads of Department Components and United States Attorneys, 12-15, available at http://www.usdoj.gov/dag/speech/2006/mcnulty_memo.pdf.
44 See *Commodity Futures Trading Comm'n v. Carnegie Trading Group, Ltd.*, 450 F. Supp. 2d 788, 804-05 (N.D. Ohio 2006).
45 See *W.G. Yates & Sons Constr. Coo., Inc. v. OSHA*, 459 F.3d 604, 608-09 (5th Cir. 2006).
46 429 U.S. 589 (1977).
47 Ibid., 591.
48 Ibid., 593.
49 Ibid., 17. The appellees also challenged the efficacy of the database. For example, while a search of the records would identify a person who obtained multiple prescriptions under the same name, it could not detect a person who used an alias to obtain the prescriptions.
50 Ibid., 593-94.
51 Ibid., 605-06 (emphasis added).
52 Posner, *Suicide Pact*, 37.
53 See *Kolstad v. American Dental Ass'n*, 527 U.S. 526 (1999) (good faith compliance efforts can be a defense to punitive damages liability in federal civil rights action); *Burlington Indus., Inc. v. Ellerth*, 524 U.S. 742 (1998) (reasonable efforts to detect and remedy incidents of sexual harassment can be defense to employer liability); *Faragher v. City of Boca Raton*, 524 U.S. 775 (1998) (same).
54 See *Stone v. Ritter*, 911 A.2d 362 (Del. 2006); In re *Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).
55 *Youngstown*, 343 U.S. at 635 (Jackson, J., concurring in the judgment and opinion of the Court).
56 See Posner, S*uicide Pact*, 9.

A . A A B B

The leaders of Southern Methodist University believe that a university does not fully discharge its responsibility to its students and to the