IX. The Complexities of Oversight and Accountability

Assuming that there are ways of aligning the values that infuse various liberal democratic societies, there is still the important question of how to implement them within the diverse institutional arrangements in which they are or will be embedded.[1] What regulatory or oversight arrangements would be most suited to their realization?

Ideally, oversight arrangements within liberal societies will reflect their undergirding values. Oversight mechanisms should gravitate in the direction of structures that exemplify those values. In particular – and apposite to the concerns of this study – there will be a determination to ensure social arrangements in which personal accountability is both fostered and maximized.

However, as liberal writers from as far back as John Locke have realized, good social order requires more than reliance on individual good will and good judgment. Structural supports and incentives are needed. As civil society itself exemplifies – with its legislative, judicial and enforcement structures – the human condition requires more formalized approaches to social ordering than a *laissez faire* expectation will be able to deliver. Even so, more formalized approaches can differ significantly in the level of compulsion they involve. Although we noted in Chapter IV of this study the need and our desire to eventually move the US in the direction of creating an independent National Office of Data Protection, we understand that traveling this path is likely to be slow going. Recognizing this reality, our inclination here is therefore first of all to advocate for better development of what we term a "soft-law" approach to accountability. We recommend this tactic in conjunction with the development of appropriate legislation and enforcement mechanisms. Ultimately, in this area as elsewhere, there is a need for an integrated mix of soft law and coercive hard law.[2]

[1] The Appendix provides some insight into the complexity of implementing common global standards for security and privacy, even within liberal democracies. Reviewing the variety of institutional structures and oversight mechanisms established by Australia and India gives perspective to the wider challenge beyond that posed by the EU–US focused discussion that has primarily occupied us.

[2] We are mindful of T. H. Green's warning – albeit in a somewhat different context – that the precise measures to be adopted as social policy need to have regard to what people will tolerate: "to attempt a restraining law in advance of the social sentiment necessary to give real effect to it, is always a mistake." See T.H. Green, "Liberal Legislation and Freedom of Contract", (1881), published in *Works,* ed. R.L. Nettleship (London: Longmans, 1888), vol. 3, 265–86. The Appendix to this study adds grist to this mill. The countries reviewed clearly operate at different points of what could reasonably be construed as a security/privacy continuum. Recognizing that such variation exists requires sensitivity in establishing mechanisms for achieving the common end of desired protection for multiple stakeholders. Providing a flexible framework for choosing and implementing a menu of means, which we are attempting to articulate here, is essential to enabling success in what are often dissimilar settings.

A soft-law approach to enhancing oversight can serve as an intermediate mechanism for managing already legislated or regulated surveillance activities where guidance for achieving accountability is vague and where the political will to clarify confusion is not exercised. It can also be useful in cases in which emerging surveillance issues require clarification before hard law is explored and introduced. The recommendations that we make in this chapter focus specifically on increasing accountability in electronic surveillance, profiling and data mining efforts through the utilization of an accountability assessment tool that allows an organization to take stock of its surveillance operations, and through the creation of multi-disciplinary Techno-ethics Boards that could be worked into the process of building and applying surveillance programs.

Soft law and oversight

To date, hard law has served as a less-than-ideal means of achieving accountability in surveillance operations across levels of government in the US and elsewhere. Although such legal tools hold a necessary place among the approaches to monitoring and controlling surveillance operations, even after long and detailed public discussion (resulting in actual laws and codified rules of implementation for techniques such as wiretapping), they have nevertheless sometimes proven ineffective in certain areas of practice. Such failures of foresight have required the employment of effective practical oversight methods so that problems that have emerged can be identified and rectified. As a recent example, we need look no further than the dilemmas that the FBI has encountered with its surveillance activities. Although the USA PATRIOT Act authorized the use of National Security Letters (in effect, administrative subpoenas) by the FBI in investigations of international terrorism and foreign spying,[3] a Department of Justice Office of Inspector General (OIG) report indicated that in the earlier part of this decade there had been insufficient monitoring of the implementation of this strategy by its field officers. These findings raised questions of impropriety and illegality in the FBI surveillance activities that had been implemented.[4] It was fortunate that this step was taken by the OIG before problems found their way into the court system for settlement through judicial review of administrative operations. It is just this type of occurrence that points out the weaknesses and openings for abuse that can arise between the development of hard law and its resulting implementation. As we have previously noted, another problem that has

[3] See Charles Doyle, "National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent Amendments", *CRS Report for Congress Received through the CRS Web*, March 31, 2006, Order Code RS22406.

[4] See Julie Hirschfeld Davis, "Lawmakers Warn FBI Over Spy Powers Abuse", Associated Press, March 21, 2007.

come to light involving the FBI regards the illegal soliciting of phone records between the years 2002 and 2006.[5] A Justice Department OIG report examines these issues in depth.

In other situations, developers of hard law can find themselves struggling to offer the insight required to do the job of managing surveillance activities effectively where newer forms of technology are involved. This too can result in problems developing during implementation that will not be rooted out early, and are left to be caught only after they have impacted upon the public. For example, unique expertise that exists among private sector professionals developing technology and innovations within certain fields, such as facial recognition imaging, enables them to operate at such high levels that without commensurate knowledge at their disposal government regulators and elected officials may find themselves challenged to create well-targeted and effective control mechanisms within legislation. Understanding these shortcomings, a more flexible means of ongoing oversight needs to be sought out that can provide stability as the development and eventual implementation of hard law requirements are pursued.

One approach to shrinking this gap in effectiveness and accountability is to heighten flexible governmental regulation and oversight activities through the exploration of "soft law". Discussions of soft law can be considered part of an emerging discourse on the overall value of regulation and governance that in academic circles has recently come to the foreground in a multi-disciplinary fashion.[6]

"Soft law" is an inexact term that covers a multitude of quasi-legislative, often non-binding instruments used to enhance government efforts to regulate service delivery areas. These instruments are intended to enable policy changes to emerge and harden through voluntary application and adherence in both confrontational and politicized atmospheres in which a wide array of players from public, private and non-governmental sectors are involved.[7] Such tools have been referred to broadly as "unofficial guidelines" that deliver information to those being regulated.[8]

[5] See John Solomon and Carrie Johnson, "FBI Broke Law for Years in Phone Records Searches", *The Washington Post*, January 19, 2010, A01. Additional information about the role of the ill-fated White House Privacy and Civil Liberties Oversight Board in this case can be found in Allen Charles Raul's Letter to the Editor, "The Missing Privacy and Civil Liberties Oversight Board", *The Washington Post*, January 24, 2010.

[6] See John Braithwaite, Cary Coglianese, and David Levi-Faur, "Editors' Introduction: Can Regulation and Governance Make a Difference?", *Regulation & Governance* 1 (2007): 1–7.

[7] See Taco Brandsen, Marcel Boogers, and Pieter Tops, "Soft Governance, Hard Consequences: The Ambiguous Status of Unofficial Guidelines", *Public AdministrationReview* 66, no. 4 (July/August 2006): 546–53; and Peter Mameli, "Managing the HIV/AIDS Pandemic: Paving a Path into the Future of International Law and Organization", *Law & Policy* 22, no. 2 (April 2000): 203–24.

[8] Brandsen, Boogers and Tops, 546.

Some of the instruments that communicate these ideas include codes of governance, quality standards, letters of advice, handbooks, manuals, reports, declarations, recommendations, guidelines and resolutions, to name a few.[9] They can be used to fill gaps between existing legal norms and implementation shortcomings, or to exercise initiative where no legal guidance currently exists. The result is intended to be a collaborative effort at ensuring quality service delivery by all parties involved in the process. Sometimes they can even result in the drafting of enhanced or new binding legal agreements, after a slow process in which policy diffusion is accepted and validated by the players affected.

In the case of government surveillance programs that rely on electronic surveillance, profiling or data mining activities, construction and delivery of mutually acceptable soft-law guidelines for their ongoing management and oversight would likely enhance reliability in the eyes of the public. Among the guidelines provided could be agreement to the need for time-driven audits and program evaluations, ongoing development of relevant performance measurement indicators, public reporting expectations on the results of the measurement systems created and the use of Techno-ethics Boards to resolve issues of ethical concern at the same time as developing advice for carrying out surveillance activities from the beginning of operations through to their conclusion. These ideas will be expanded on in later sections of this chapter.

Soft governance, trust and success

Although a soft law approach to oversight promises to relieve problems and pressures that have surfaced with surveillance programs, there are also quandaries to address well before such programs are productively employed. Quasi-legislative instrumentation of the nature discussed here is voluntarily adhered to and presents an uncertain edict to those on the receiving end. The intent is obvious; the authors of soft law believe that others should follow these "suggestions" and upgrade their operations accordingly. Yet there is no "authority" determining that action be taken. These are not new laws or regulatory rules that must be followed. They are something else: important enough to be taken note of, but ignored at one's own professional and personal peril.[10] Complicating matters further, soft law often suggests that new implementation norms be followed and attested to through self-reporting by the entities that are charged with providing a particular service. Yet, given

[9] Brandsen, Boogers and Tops, 546; and Mameli, 203.

[10] Brandsen, Boogers and Tops, 550–51.

that a gap exists between hard law and regulation and implementation in this sensitive policy area, a soft-law approach does offer opportunities to begin the process of deepening oversight.

The conundrum noted above frames a central discussion point that needs to be entertained here: how does soft law consistently result in something more than soft, or even abdicated, governance? Even if governance was found lacking before, does this yield a better answer? How can you be sure you have not let the fox guard the henhouse when you are counting on the fox to give you a daily testament to his/her actions? Given this problem, it is important to begin by noting that there are two sides to the coin of soft law.

The first side of the coin views the use of such unofficial guidelines as necessary tools for distributing new information to agents perceived as needing to update and improve their services, while still creating room for innovative practices to flourish. This view assumes good faith on the part of those being regulated to honestly address the suggested course of action, or to offer a better path to follow. The other side of the coin is one in which the suggested changes are not implemented due to a lack of comprehension or ability on the part of the receiver, a lack of leverage on the part of the sender or, worst of all, a desire by one or both to engage in fraud, waste or abuse by keeping loopholes open and outside eyes closed.[11] Both sides of the coin are relevant parts of the discussion about the implications that these instruments have for practitioners of soft law in complex environments.

When constructed well, the use of soft law to close gaps between hard law and implementation efforts opens doors to programmatic innovation and improvement. In practice it can also serve to increase accountability by mitigating administrative confusion and folly due to imprecise understandings of how to accomplish desired ends. However, it is also true that political stressors and unclear messages from central authorities regarding unofficial guidelines can drag down the potential gains of the process by causing those being regulated to stifle innovation and simply toe the line in order to avoid being cited during inspections and oversight – even though these are not clear infractions that they will be called on.[12] In such a scenario, the process that should lead to an active interchange of ideas between the center and the periphery that results in continuous improvement leads only to a game of follow-the-leader or, worse, resistance. Further still, poorly developed unofficial guidelines that do not provide effective problem resolution can also allow for abuse in application by practitioners.

[11] See *Ibid*, 547–48, for a nice breakdown of possible paths that regulated parties can take in reaction to unofficial guidelines.

[12] *Ibid.*, 550–51.

We should be striving to shut off the mains that allow illegal activity to flow forward by crafting useful soft law that also improves results. In the world of surveillance operations such a goal is of great value in and of itself, given the threats to liberty, privacy, and civil rights that hang in the balance. The question that emerges becomes: How can the relationship between those sending the soft forms of guidance and those receiving it be made to work better? Can we ensure transparency, attain accountability, improve effectiveness, prevent misconduct and enable innovation all at once? Can individuals charged with overseeing government surveillance programs help this development along in a front-to-back process? The answer seems to boil down to partnership and how to achieve it.

If creative interchange between all parties is what is desired then trust must be created to allow the interchange to flourish. That trust needs to run through the entire process. Trust must exist in the formulation of the quasi-legislative instruments and advice up front, as well as in the oversight process that is created afterward. However, it is hard to create that level of trust when there is resistance to oversight in sensitive areas of national security (e.g. involving surveillance operations, or any other activity).

Certainly, recent problems between the US CIA and its own OIG, where the former challenged the investigative methods of the latter in politically sensitive reviews, attest to this dilemma.[13] Indeed, at this time the agency has successfully managed to create two new positions to oversee the actions of its own internal watchdog![14] Yet oversight and accountability of national security activities must exist, and so the conundrum surrounding trust is laid bare. One undeniable finding from the CIA's situation so far is that at the very least a lack of trust in oversight operations distracts an organization from accomplishing its mission. Therefore, if government is to function effectively it seems clear that trust needs to be established early on rather than as an afterthought or as the result of a crisis.

In unpacking these concerns we first examine weaknesses that complicate the processes of soft law implementation and then note how particular forms of collaborative (rather than adversarial) interaction between oversight entities and those being inspected can improve accountability through enlightened, triangulated oversight. In conjunction with this analytical effort, addressing elements of performance measurement and management that can be used in constructing transparent and accountable partnerships between oversight agents and those being inspected must be further developed. Taken in total,

[13] Mark Mazzetti and Scott Hane, "CIA Watchdog Becomes Subject of CIA Inquiry", *The New York Times*, October 12. 2007, A1, A25.

[14] Greg Miller, "CIA Places Controls on Inspector General", *Los Angeles Times*, February 2, 2008, retrieved February 9, 2008 at: www.latimes.com/news/printedition/a/la-na-cia2feb02,1,6583760.story.

our recommendations represent an attempt to stretch the current discourse on regulating new and existing surveillance operations into less-well-traveled areas of thought. Here we are considering a role for oversight personnel in government surveillance that is essentially counter to the logic of reaction and punishment that often permeate such dialogues, and then offering tools to build trust between these parties and enhance capacity to achieve success. It may be hoped that the framework we lay out here can create room for free thinking and discussion about soft law in regard to better managing the surveillance society of the future.

Surveillance technology accountability assessment tool

What we initially offer below is a soft accountability assessment tool, designed to encourage those who engage in surveillance, data mining and profiling, to reflect on the nature and consequences of what they are doing. In many respects it particularizes the various means-end questions that we raised at an earlier stage of this discussion, linking those questions specifically to what we can characterize broadly as surveillance technologies.

The rationale behind such a tool is that within a liberal society we ought to encourage surveillance strategies that acknowledge, draw upon and foster the dignity of those who use them as well as those who are subject to them. This we do when we implement strategies that encourage individual accountability rather than presume a lack thereof. If these fail, harder strategies should be available to ensure that important liberal values are not left vulnerable and unprotected.

In addition, this tool brings focus to the channels by which oversight can be exercised on surveillance programs in order to grow accountability and ensure that reasonable levels of control and scrutiny are met.[15] Activities such as improved contracting requirements, audits, inspections, program evaluations and the establishing of ongoing performance measurement and management systems can all aid in this effort. Ingrained within the logic of the "new public management" is a heavy reliance on these practices to aid in the effective steering of government programs as they navigate the real world flows and barriers that cross the ship of state's path.[16] Bringing these concepts to bear on surveillance programs is both proper and necessary. However, though

[15] See Donald F. Kettl and James. W. Fesler, *The Politics of the Administrative Process,* fourth ed. (Washington, D.C.: CQ Press, 2009), 9–12 for a useful description of the layers of government accountability.

[16] Donald F. Kettl, *The Global Public Management Revolution,* second ed. (Washington D.C.: The Brookings Institution, 2005), 17–18.

it is essential to understand the methods for achieving and maintaining accountability, the way in which they are executed is also crucial to their success or failure.

Some of the modes of oversight noted above can be used upfront in the development of surveillance programs (strict requests for proposal and contracting requirements as well as formative program evaluations), while others can be carried out during the life of surveillance operations (performance and financial audits, interim and summative program evaluations and performance measurement reporting). The problems arise with the willingness and ability to build these activities into the entire lifespan of surveillance programs across levels of government. For instance, it is not at all clear that such oversight activities are legislatively mandated into government surveillance programs, or are expected to happen in regular patterns in all law enforcement and intelligence agencies. In addition, even if such oversight of surveillance operations is taking place, the degree to which there is regular reporting to elected officials and the public no doubt varies. Is such reporting simply desired and left to occur at the will of the agencies and oversight bodies involved, or mandated and handled in a more regimented fashion? It appears that, due to the need for operational secrecy, the former is the case more often than not, and this needs to change. The question is how to create change and enhance accountability without endangering the effectiveness of the surveillance program in question? To this end we offer a tool that will allow for self-assessment in order to begin the process of improvement in oversight and accountability activities. The tool can be used by practitioners of surveillance interested in growing accountability within their organizations, as well as those interested in carrying out oversight of these groups.

SURVEILLANCE TECHNOLOGY ACCOUNTABILITY ASSESSMENT TOOL*

1. What external agencies are charged with carrying out oversight of the creation and use of the surveillance technologies you work with? Please name the oversight agencies and explain their roles.
2. What internal units within your agency are charged with carrying out oversight of the creation and use of the surveillance technologies you work with? Please name the oversight units and explain their roles.

3. How is oversight carried out for the surveillance technologies you create and/or work with? Please explain for each condition noted below and differentiate by type of technology or method if necessary. Also, please provide documentation if possible.

   (A) Consultation with experts beyond the organization?

   (B) Closed/open meetings within the organization?

   (C) Closed/open hearings with the public or an oversight body?

   (C) Closed/open hearings with the public or an oversight body?

   (D) Program evaluations of success in implementation?

   (E) Performance audits for accountability?

   (F) Financial audits for accountability?

   (G) Investigations of fraud, waste, abuse and mismanagement?

   (H) Performance measurement and management system development and monitoring?

   (I) Other.

4. Are experts external to the organization utilized to ensure that the surveillance technology being constructed and/or utilized satisfies appropriate ethical concerns for development and implementation? Please explain. What about regulatory concerns? Please explain. What about statutory legal concerns? Please explain.

5. if your agency issues a Request for Proposal (RFP) for development of a surveillance technology, or employs a subcontractor for such a purpose, what accountability mechanisms (if any) do you require to be built into the resulting submissions to provide service? Please explain.

6. Does your agency establish performance measures in its contracts when dealing with the creation of surveillance technologies by outside parties?

   If yes, please explain the steps, benchmarks and measures that are to be built into the contract for provision of such services to determine if a vendor is effectively achieving desired outcomes.

   If you do currently establish performance measures in contracts in which surveillance technologies are created, how do you think this process could be improved?

   Finally, please explain what happens if a vendor or subcontractor fails to perform adequately.

7. Has your agency established performance measures for methods of using surveillance technologies?

   If yes, please explain the steps, benchmarks and measures that are used to monitor such services and determine if the process is effectively achieving desired outcomes. If necessary, differentiate by type of surveillance technology.

   If you do currently establish performance measures for methods of using surveillance technologies, how do you think this process could be improved?

   Finally, please explain what happens if performance is inadequate.

8. Does your agency have an articulated rule defining inappropriate and/or personal use as it relates to surveillance technologies? If yes, please explain and/or provide a copy of the rule(s).
9. Suppose that someone is suspected of misusing surveillance technology; is there a formal process for investigating and adjudicating the breach? If yes, please describe the process and/or provide a written copy of it.
10. What systems do you have in place for actively detecting potentially inappropriate or personal uses of your surveillance technologies? Please explain how this is done and whether you utilize an automatic alerting of suspected misuse systemically.
11. What systems do you have in place for passively detecting potentially inappropriate or personal uses of your surveillance technologies? Please explain how this is done and whether you have established a system of "whistle blowing" protections for people so that they feel they can alert managers and other relevant parties when misuse is detected.
12. If you work with third-party vendors to build and implement new or enhanced surveillance technologies, how does your agency ensure that the vendors and their employees do not re-use or re-sell the code for creating the resulting systems that are developed?
13. How does your organization secure proprietary algorithms for its surveillance technology activities? Please explain and/or provide written copy of the process.

14. If your organization procures third-party algorithms for surveillance technology do you have a process for checking the validity and reliability of the algorithms? If yes, please explain and/or provide written documentation of how this process would work.
15. If your organization procures data from third parties how are they securely stored when the original purpose for its use is completed? Please explain and/or provide written documentation of this process.
16. Considering how information and databases can be re-purposed and mined for an indefinite number of applications, how do you ensure that the systems you create do not exceed their legal or ethical boundaries after implementation? Please explain and/or provide written documentation of this process.

* This tool was developed by Peter Mameli and Vincenzo Sainato.

If the foregoing soft law questions are diligently asked and responded to by either internal or external parties, we might expect that liberal values will be sustained at an acceptable level. Nevertheless, it is acknowledged that a culture supportive of such an approach is not easily achieved or sustained, especially in times of apparent crisis. Therefore, various "harder" approaches may be required.

Harder approaches may take various forms. Some may take the form of (a) building ("hard-wiring") appropriate values into the surveillance technologies themselves; (b) imposing various administrative or civil penalties on those who disregard or contravene such values; and, as a last resort, (c) implementing criminal mechanisms in cases in which such values are egregiously flouted.

For a culture supportive of oversight and accountability to take root, trust must be ingrained among the parties involved. Trust can be developed in a number of ways at the beginning of operations when advice is crafted and distributed to surveillance practitioners in soft or hard forms. The first way is to utilize the accountability assessment tool provided to ease concerns that issues of oversight are being glossed over or ignored. An additional layer of protection offers the opportunity to bring a variety of parties together early in order to craft mutually agreeable guidance on surveillance operations. Such an approach could accomplish this goal in a number of ways. One is where the public sector defers to nongovernmental parties from the start in the development of said guidelines.[17] This is similar to a model of rulemaking that Weimer refers to as

[17] Brandsen, Boogers and Tops, 552. For additional examples, see Steven Bernstein and Benjamin Cashore, "Can Non-State Global Governance Be Legitimate? An Analytical Framework", *Regulation & Governance* 1 (2007); 347–71.

"private rulemaking".[18] It is important to note that the private rulemaking model is different from the "negotiated rulemaking" approach, in which external parties engage in the process but do not control it, or the "agency rulemaking" approach, in which experts and advisory boards are invited in only to offer their insight and support.[19] Each of these approaches can create buy-in early on that will help to support positive relationships as problems arise in the future. However, neither fully addresses the negative reactions to oversight discussed earlier that follow once guidance is provided. Another level of trust needs to be developed in order to get over this hurdle, and it is incumbent on the personnel charged with such oversight to help facilitate that trust. But how can this goal be achieved when thinking in the world of inspection is colored by expectations of adversarial relationships rather than collaborative ones?

Techno-ethics Boards: guiding and growing accountability

One way to build trust between practitioners and oversight entities involved in responsibly carrying out surveillance operations is to explore the creation of a means of constructive engagement between the parties. However, the form of interaction must include those who would be involved in such a process from front to back. To achieve this purpose we suggest developing Techno-ethics Boards. Akin to Institutional Review Boards (IRBs) in universities, and Bioethics Boards in health settings, Techno-ethics Boards in law enforcement and intelligence settings would be charged with advising surveillance practitioners on how to go about implementing hard law and regulation on these matters. They would also be responsible for addressing ongoing questions of acceptable practice that would evolve as technology (and criminality) changes. However, as opposed to IRBs, they would not have the ability to prevent the implementation of official policies existing in surveillance programs. Due to the need for security and the sensitive nature of information that may need to remain protected even from the board itself, final calls on implementation would still remain with law enforcement and intelligence personnel directly involved with the activity. Hence, the board's oversight of said surveillance operations would still have limits. Yet this additional layer of scrutiny would no doubt aid in clarifying problems and halting preventable errors through the application of mutually accepted soft governance, built on soft law and soft instrumentation.

[18] David L. Weimer, "The Puzzle of Private Rulemaking: Expertise, Flexibility, and Blame Avoidance in U.S. Regulation", *Public Administration Review* 66, no. 4 (July/August 2006): 569–82.

[19] *Ibid.*, 569.

IRBs have been used within universities for decades to protect human and animal subjects from research abuses.[20] Although the protections of subjects and procedures for construction of a Techno-ethics Board to provide guidance to government surveillance programs might indeed differ from an IRB, it is a worthwhile enterprise to begin exploring. Could such a body stop abuses from happening in cases in which law enforcement and intelligence efforts are trying to protect national security but go beyond acceptable norms of practice? If so, it is at least worth the effort to take a close look at the possibilities for such boards. Why risk making the error of creating a new type of Stanley Milgram scenario, where both surveillance practitioners and their subjects become victims of overzealous observation efforts, if it can be short-circuited?[21]

As with federally mandated IRBs a Techno-ethics Board would require a spray of appropriate expertise and talent, with a recommended membership of at least five parties.[22] The members would include, at a minimum, one lawyer, one ethicist, one technology expert, one oversight expert and one field practitioner. As with IRB appointments, sensitive demographic information would also need to be taken into account in the development of a Techno-ethics Board in order to ensure that a balance of backgrounds is represented.[23] All may come from government circles, or none. However, there are complications that come with including non-governmental entities in security driven operations that make for a quandary in this regard. It is more likely that, given the information and the context under which surveillance reviews would take place, personnel would need to be drawn from across differing law enforcement agencies (and perhaps levels of government) more so than from outside parties. However, regardless of who is chosen to serve, the goal would not be to create a confrontational atmosphere but rather a mutually supportive one in which professionals concerned with surveillance and its implications could gather to address real-world implementation issues.

Evaluating the difficult choices that must be made by governmental entities, in which adherence to protections of civil rights and liberties are traded against the need for protection, is no easy task. Given that matters of security are at stake, parties granted entrance to a given Techno-ethics Board at any level of

[20] Lawrence W. Neuman, *Social Research Methods: Quantitative and Qualitative Approaches,* fifth ed. (Boston, MA: Allyn and Bacon, 2003). Recently Christine Grady surfaced concerns about the effectiveness of IRBs in her article entitled, "Do IRBs Protect Human Research Participants?", *Journal of the American Medical Association* 304, no. 10 (2010): 1122–23. A key point made was that a lack of evidence exists allowing such a question to be resolved, and that new approaches to measure the work of IRBs must be developed. Clearly, the best way to build a Techno-ethics Board would be to benefit from the improvements in IRBs that will likely be generated from the ensuing discussion of Grady's comments.

[21] Royce A. Singleton, Jr. and Bruce C. Straits, *Approaches to Social Research,* fourth ed. (NY and Oxford: Oxford University Press, 2005), 519.

[22] Singleton and Straits, p. 530.

[23] Elizabethann O'Sullivan, Gary R. Rassel, and Maureen Berner, *Research Methods for Public Administrators,* fifth ed. (US: Pearson Longman, 2008), 261.

government should not be chosen without careful consideration. As such, it is important to turn to those who have the levels of clearance necessary to be involved with these matters. One such participant could be found within OIGs. OIGs have already been awarded oversight responsibility at the federal level of surveillance operations in the US through the Foreign Intelligence Surveillance Act Amendments Act of 2008. Considering personnel from these organizations for inclusion within a Techno-ethics Board is therefore no great leap of logic. Now that the OIG concept is found in many countries around the world and operates at many levels of government, OIG members would constitute a good population to explore for the purposes of this discussion.

By taking some time to look at the theory that underpins OIGs in the US we can begin to see how one type of inspection and oversight body's personnel can be deployed constructively and justifiably in a Techno-ethics Board. If welded together carefully with other relevant members, surveillance practitioners can be provided with a feeling of comfort that they remain free to innovate solutions to crime and intelligence problems despite the existence of the board. Further still, they will feel that they have somewhere to go for support and guidance as the inevitable tough decisions arise.

Offices of Inspector General and Techno-ethics Boards

Over the last twenty years in the US, OIGs have become common entities on the government oversight landscape. With a growing realization that the costs of corruption and abuse devastate all sectors of society, there has been an increasing reliance on oversight bodies such as OIGs to step up and ensure accountability and transparency. Yet OIGs do not need to be only reactive in their work, seeking out wrongdoers for punishment after infractions have occurred. OIGs can also be proactive and can become engaged in constructive efforts to ensure that processes of change occur smoothly and, in select circumstances, that innovation is encouraged without fear. As such, there is an increasing role for OIGs in facilitating soft governance by engaging in a type of consultative capacity building that can enhance oversight.

OIGs have a straightforward purpose that is reflected in the US Association of Inspectors General's (AIG) explanation of its role:

> Accountability is key to maintaining public trust in our democracy. Inspectors general at all levels of government are entrusted with fostering and promoting accountability and integrity in government. While the scope of this oversight varies among Offices of Inspectors

> General (OIGs), the level of public trust, and hence public expectation, embodied in these offices remains exceptionally high. The public expects OIGs to hold government officials accountable for efficient, cost effective government operations and to prevent, detect, identify, expose and eliminate fraud, waste, corruption, illegal acts and abuse.[24]

The AIG further notes that the qualifications and skills that should exist in these offices include:

> Skills needed to evaluate the efficiency, economy, and effectiveness of program performance within the OIG's area of responsibility . . . and state-of-the-art technical skills as needed such as computer auditing, detection of computer fraud, review of information technology design requirements, statistical sampling and analysis, factor analysis, trend analysis, systems and management analysis, undercover techniques, and covert surveillance.[25]

The language above casts OIGs in a reactive oversight role to those they are overseeing. This role has most recently been seen in the efforts of five federal OIGs to examine the President's Surveillance Program as required by the FISA Amendments Act of 2008.[26] However, the work of OIG staff does not have to be restricted to post-implementation analysis once they become part of a Techno-ethics Board. Where compliance efforts are voluntary to start with, rather than mandated, members of OIGs working on Techno-ethics Boards can take on more of a capacity-building face than they might normally do when they maintain their regular oversight watches. In fact, the skills identified above can be put to use in a multitude of ways so as to build operational understanding as part of a Techno-ethics Board's abilities. Expertise brought to the table by OIG personnel can enhance adherence to unofficial guidelines upfront, or can at least increase understanding of why such guidelines are being ignored or improved upon by the parties being asked to implement them. Under such a rationale, members of OIGs on Techno-ethics Boards could view themselves as being in position to get ahead of problems, rather than be trapped behind them. The parties being asked to conform to such soft-law advice would feel that they are being worked with, rather than being worked over. This would be especially true if surveillance practitioners were given time to comment on board advice prior to it being finalized and recommended. In addition, OIG personnel would not find themselves totally out of the loop as implementation (or the lack of it) moves forward. Finally, when OIG personnel on Techno-ethics Boards receive the self-

[24] Association of Inspectors General, *Principles and Standards for Offices of Inspector General, 2004* (Philadelphia: Association of Inspectors General, 2004).

[25] *Ibid.*

[26] Offices of Inspectors General, *Unclassified Report of the President's Surveillance Program – Report No. 2009-0013-AS* (Washington, D.C., 2009).

reported attestations of those being overseen, they will have a much better understanding of what is being presented in the final documents. The ways in which they would then address issues of non-compliance and enforcement could proceed with greater understanding.[27] Similar benefits would likely be gained by all participating members of a Techno-ethics Board.

In this chapter of the study we are suggesting that creative soft-law approaches to government surveillance programs can supplement – and in some cases, obviate the need for – hard law by successfully addressing and containing abuses of power that occur through negligence, overzealous application or outright abuse. They can also aid in simply containing random error. The utilization of the Surveillance Technology Accountability Assessment Tool to assess current surveillance oversight practices, and the creation of intermediary bodies such as Techno-ethics Boards that can be used to provide advice and guidance at points between those who create hard law and regulation regarding surveillance operations and those who practice its implementation, are the touchstones of this offering. Future research in this area should, at the very least, explore: (1) The possibilities for such enterprises to be developed; (2) The procedural hurdles that would need to be overcome to make Techno-ethics Boards a reality in law enforcement settings across levels of government; (3) the selection of proper participants in such endeavors; and (4) the piloting of the Surveillance Technology Accountability and Assessment Tool in a variety of settings to determine its overall usefulness.[28]

[27] See Christopher S. Decker, "Flexible Enforcement and Fine Adjustment", *Regulation & Governance* 1 (2007): 312–28, for some private sector examples.

[28] Vincenzo Antonio Sainato's criminal justice dissertation, "Situational Surveillance Control" (City University of New York, John Jay College of Criminal Justice, 2009), explored the value of this tool as part of an ethnographic examination of the Branford, Connecticut, Police Department.