X. Recommendations

Here we articulate a series of recommendations with respect to the use of technologies identified in Chapters VI and VII that will bear on both accountability mechanisms and legal constraints/requirements. Although these recommendations focus particularly on the current US situation, they have clear implications for democratic polities writ large. To some degree, our recommendations arise out of a review of the EU experience which, even if flawed in the implementation, strikes us as formally well-developed.

(1) That steps be taken to make the American public more aware of the extent to which its expectations of privacy have been compromised.

The point here is that compromises of individual privacy – via the collection of data by government agencies – are not limited to newspaper exposés such as those undertaken by the *New York Times* but are a much more pervasive feature of contemporary life, engaged in not only by government agents but also by private information-gathering firms. Further, these gathered materials are in many respects vulnerable to unauthorized access by others via hacking, non-encryption of databases and so on. Despite the willingness of individuals to make private personal data known to others via social networking sites, we believe that if awareness of the extent to which personal data is available, accessible and collected is raised there will be an increased concern about privacy and the extent to which it has been compromised. One opportune time to initiate a more visible national discussion would be the next International Data Privacy Day, currently celebrated on January 28 of each year. If a coalition of data protection advocates, private sector organization representatives charged with protecting privacy, and public officials engages in the concerted promotion of such a dialogue, it will constitute a good first step in this direction. Using this opportunity to begin debate on the recommendations of this study would allow for a more focused conversation to surface on security and privacy than we have seen to date.

(2) That this process draw attention to the collapse of the traditional distinction between the commercial and governmental collection, use and retention of personal data.

We are particularly concerned – especially in the case of the US – that it be made known to what extent a traditional division between the government's access to private data and commercial access to that data – for legitimate commercial purposes – has broken down, in order that there will be increased concern about issues of privacy and the legitimate expectations that we may have concerning its protection. The relationship between these growing infringements on information privacy and the resulting uses of data by law enforcement, intelligence and national security organizations should be highlighted as a part of the ensuing activities.

(3) That this process also include a clear articulation of the values that inform personal privacy, and that this extend to expectations of privacy in public.

Along with an increased awareness of the extent to which private data are now widely available – and of course the various uses to which they are and may be put – we believe that there should also be more public articulation of the importance of privacy to individual and social wellbeing, to the preservation of dignity and to the securing of our identities as citizens in a liberal democracy. Recent revelations of how the New York Police Department's Intelligence Division has worked with the US CIA to engage in questionable domestic surveillance operations indicates how urgent it is to engage in this clarification.[1] Given the current terrorist threat environment, brighter lines of demarcation must be drawn to separate acceptable and unacceptable impacts on these values.

1 Adam Goldman and Matt Apuzzo, "With CIA Help, NYPD Moves Covertly in Muslim Areas", Associated Press New York, August 24, 2011, available at: http://abcnews.go.com/Politics/wireStory?id=14368992.

(4) That there be greater transparency regarding the kinds of data digitally collected, stored and used.

Transparency is a significant liberal value, and a liberal democratic society that lacks transparency is seriously compromised. Although we do not doubt the importance of the challenge posed by transnational crime and terrorism, we believe that responses to it should be conducted in ways that do not unnecessarily compromise the privacy, autonomy and ultimately the dignity of citizens. That will happen only if there is transparency about how those who represent us in government are transparent about what personal data are collected and how they are being used. To this end, we recommend that government agencies construct and publicly report on performance measurement indicators within their organizations' performance management systems that clearly display activities in these areas.

(5) That a national public discussion be initiated concerning the legitimate extent and limits of privacy, and of ways of protecting it.

We believe that social changes have significantly affected the nature and extent to which the privacy of citizens is construed and secured, especially (though not exclusively) as a result of technological advances and their deployment to counter crime and terrorism. We believe that these changes need to be publicly acknowledged and discussed as part of the deliberative life of a liberal democratic community.[2]

2 Recent discussions in the UK and the US about limiting the use of social media sites during times of political and social unrest display the need for early reflection on such concerns. Decisions relating to restricting free speech in these contexts could lead to a future erosion of privacy rights in others. Although they are not dominoes, many issues intersect with the way in which we construct our image of privacy. Waiting for riots and protests to break out in order to address such complexities is akin to closing the barn door after the horses have already fled. See James Robinson, "Twitter and Facebook Riot Restrictions Would Be a Mistake, Says Google Chief", Guardian.co.uk, August 27, 2011, available at: http://www.guardian.co.uk/media/2011/aug/27/twitter-facebook-riot-restrictions-eric-schmidt. See also Daniel B. Wood, "BART Puts Social Media Crackdown in Uncharted Legal Territory", *The Christian Science Monitor*, August 16, 2011, available at: http://www.csmonitor.com/USA/Justice/2011/0816/BART-puts-social-media-crackdown-in-uncharted-legal-territory.

(6) That the US federal government create a National Office of Data Protection (NODP) charged with responsibility for developing national policy guidelines and recommendations for associated legislation for the protection of personal data, and with responsibility for oversight of compliance with such guidelines and legislation.

In part because transnational crime and international terrorism are of national concern, and also in order to avoid a piecemeal approach to an issue of national concern, we believe that a federally funded and nationally focused office should be set up to gather data concerning privacy-related issues as well as to develop national guidelines and associated legislative provisions for the protection of privacy. This office should also oversee compliance with privacy legislation and guidelines, including implementation of program evaluations, audits, receipt of complaints and investigation of infringements of privacy rights.

(7) That these guidelines and recommendations for associated legislation take into account both commercial and governmental collection, use and retention of personal data.

The NODP should see its role as encompassing all significant compromises or threats to private data, whether they are initiated by government or commercial agencies. Especially given the nexus that has developed between commercial data gatherers and governmental interests, we do not believe that the existing conventions concerning governmental and commercial or private data gathering retain any significant validity. Only an NODP charged with recommending the regulation of both public and private sector entities involved with privacy matters can adequately satisfy this need.

(8) That the NODP recommend a graduated series of guidelines and legislative provisions for the oversight of personal data collection, use and retention by private and public agencies, including but not limited to soft-law self-regulatory measures, privacy enhancement of software, administrative measures designed to protect privacy and the identification of situations in which criminal penalties ought to be levied.

Recognizing that the social history of the US is distinct from that of the EU, we believe that a graduated system, commencing with voluntary compliance with general guidelines, is best suited to the former's distinctive culture. However, we also recognize that self-regulation has had only a modest success and that it needs to go hand in glove with more coercive options given the inevitability of noncompliance.

(9) That the NODP also have a communicative responsibility to ensure that the American public is aware of current concerns about the privacy of personal data, as well as recommendations concerning protection enhancements.

It is critical to liberal democratic communities that information concerning data protection issues and contemplated responses to them be made available in fora that enable public discussion to play an effective role in reviewing problem areas and responding to them. Although some watchdog and advocacy organizations already exist for that purpose, we believe that the NODP should have a responsibility of its own for ensuring that a public debate occurs.

(10) That the NODP explore the possibility of the formation of Techno-ethics Boards to provide practical oversight of institutional data collection and surveillance operations.

It is not enough to have a general office of data protection such as the NODP; a more focused body is required to provide immediate oversight of operations that threaten privacy boundaries, whether they are engaged in by government or commercial agencies. Internal to organizations, Techno-ethics Boards have the ability to engage in proactive troubleshooting and problem solving. Where programs of data collection, retention and use, as well as surveillance and profiling, are formed and implemented, the varied expertise of board members can help to achieve and maintain a successful equilibrium between security and privacy interests.

(11) That the NODP liaise with the European Data Protection Supervisor and those similarly situated in other liberal democratic countries to develop a set of standards that can be generally implemented within such societies.

As we have indicated, there is a rich international resource of experience in data protection and oversight to be drawn upon, and though we do not question the distinctive circumstances of social and political life in the US, we believe that there is a great deal to be learned – not only by the US – through developing firm links with similar kinds of agencies in other liberal democratic societies. However, we see the purpose of such liaisons not only to be one of mutual enrichment but also as a means whereby – in an increasingly connected world – universal standards for data collection, processing, dissemination and retention can be developed.