

Center for National Security Studies

Protecting civil liberties and human rights

Director
Kate Martin

Deputy Director
Lisa Graves

April 8, 2009

Melissa Hathaway
National Security Council
The White House
Sent via e-mail

Dear Ms. Hathaway:

Thank you for meeting with us and providing the opportunity for comments for the cybersecurity review you are conducting. I hope these comments are still timely. I apologize for their tardiness and will keep them brief.

Review of applicable legal authorities.

We support the proposals for a review of the applicable legal standards. We believe such a review is needed not only to ensure that the law is up-to-date, clear, workable and consistent with security objectives, but also because changes in current laws are needed to restore traditional protections for privacy and civil liberties.

Need for review. In the past few years, the legal authorities permitting collection of information on Americans have been expanded and the limitations and safeguards against abuse have been weakened. Unfortunately many of these changes were accomplished without consideration of whether alternative measures exist that would provide the same security benefits and pose fewer threats to civil liberties. In addition, as I mentioned in our meeting, the traditional legal architecture intended to safeguard civil liberties was tied to concepts that have been substantially eroded or transformed, *e.g.*, the divide between foreign and domestic and between intelligence and law enforcement. At the same time, there have been tremendous advances in technological surveillance capabilities and a transformation in the way individuals communicate. One effect of this is that transaction information of the kind that may be quite useful for cybersecurity can be mined to be potentially as revealing of an individual's private associations and activities as the content of that individual's communications.

These changes pose challenges to civil liberties that go far beyond the risks of individual wrongdoing and misuse of personal information, such as identity theft or illegal uses of personal information by government officials. Rather, they pose challenges to the balance of power between the government and the citizens. As Senator Sam Ervin explained in 1974:

[D]espite our reverence for the constitutional principles of limited Government and freedom of the individual, Government is in danger of tilting the scales against those concepts by means of its information gathering tactics and its technical capacity to store and distribute information. When this quite natural tendency of Government to acquire

and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy makes it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom.

Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom: the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.¹

Scope of review. Such a review should include a comprehensive look at all the authorities which provide the government with access to personal information about Americans that may be relevant to cyber-security, including FISA, section 215 of the PATRIOT Act, and national security letters, which operate in tandem with ECPA and the Privacy Act. The President has indicated his intention to ask the Attorney General to conduct a comprehensive review of domestic surveillance. It may make sense to combine these reviews rather than conducting a separate review focused solely on authorities directly applicable to cyber-security issues.

Conduct of legal and policy reviews: Privacy and Civil Liberties Oversight Board.

To the extent that your review is going to endorse establishing legal and policy reviews such as those outlined in the CSIS report or the proposed Rockefeller – Snowe draft legislation, we would strongly recommend that any such review be co-chaired by the Chair of the Privacy and Civil Liberties Oversight Board. These issues are centrally entwined with protection of privacy and civil liberties and establishing co-chairs will assure appropriate consideration of the issues.

Guidelines for future legal reviews and reforms.

To the extent that your review recommends further processes for making substantive policy or legal changes implicating civil liberties, we would strongly recommend that such processes specifically require identification and consideration of alternative solutions to meet the security objectives and preference for the solution which is most protective of civil liberties and most transparent consistent with appropriate risk-management objectives.

We also urge you to recommend that any reform proposals generated as a result of your review specifically direct that greater legal protections must be accorded Americans' personally identifiable information. One way to restore Fourth Amendment protections is outlined below, which we would urge you to consider.

¹ Senator Sam Ervin, June 11, 1974, *reprinted in* COMMITTEE ON GOVERNMENT OPERATIONS, UNITED STATES SENATE AND THE COMMITTEE ON GOVERNMENT OPERATIONS, HOUSE OF REPRESENTATIVES, LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974 S.3418, at 157 (Public Law 93-579)(Sept. 1976).

Proposals for authentication requirements/ Anonymized data/ and Fourth Amendment protections for transaction information.

As you know, current proposals to consider broader authentication requirements on both private and government networks raise serious privacy and civil liberties concerns. To the extent that your review is going to endorse considering this option, we urge you to endorse simultaneous consideration of an approach that would restore Fourth Amendment protections for Americans' personal information while still meeting security needs. Doing so would ameliorate the risks to civil liberties from adopting authentication requirements.

In particular, we urge you to recommend consideration of an approach that would require technological anonymization of personally identifiable information accessible to the government on networks. While the government would be entitled to access such anonymized transactional (non-content) data without a warrant, it would then be required to meet Fourth Amendment standards in order to pierce the anonymity and obtain the personal identifiers related to the transactional data..

When the government has access to streams of network data containing personally identifiable information, the network could be required to carry such data in a way that personal identifiers may be electronically and automatically separated from the rest of the data, in effect anonymizing the stream of data. The government would be authorized to access the personal identifiers for such data only if it met Fourth Amendment standards, that is, a judicial warrant based on probable cause. As you know, Supreme Court decisions have been interpreted to mean that the Fourth Amendment does not protect transactional or third party data, so such a requirement should be statutorily imposed.

Conclusion: We very much appreciate the administration's commitment to protecting privacy and civil liberties as a fundamental part of its efforts to protect the integrity of cyber-networks. We do not believe that adequate solutions to do so have yet been identified in light of the enormity of recent technological changes and we welcome the administration's efforts to do so. We believe that the proposals outlined above may serve as a first step towards identifying such and we very much appreciate consideration of our views.

Sincerely,

Kate Martin