Why the Federal Government Should Have a Privacy Policy Office

Peter Swire[1]

These comments support the creation of a Privacy Policy Office in the executive branch, as called for in the Department of Commerce Green Paper, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework."

The chief criticism of this proposal is that the Office would weaken privacy protection. In one vivid turn of phrase, Jeff Chester of the Center for Digital Democracy said: "Having the Commerce Department play a role in protecting privacy will enable the data collection foxes to run the consumer privacy henhouse."[2] Mr. Chester and other privacy advocates essentially argue that having the Commerce Department play a role in privacy policy will dilute the effectiveness of the Federal Trade Commission's (FTC) privacy efforts.

I disagree. My comments support three conclusions:

1. The Office would provide important benefits to complement what the FTC does. As part of the executive branch, the Office would make distinctive contributions to building privacy policy into the development and implementation of U.S. government positions for domestic and international policy. Relatedly, the Office would be able to draw on the perspectives and expertise of other federal agencies far more effectively than can an independent agency such as the FTC.
2. The likely outcome with an Office would be better protection of privacy than would occur without the Office; and
3. The likely outcome with an Office would be better achievement of other policy goals than would occur without the Office.

These comments also consider whether the Office should be placed in the Department of Commerce, as the Green Paper recommends, or else in the Executive Office of the President, which housed the office of the Chief Counselor for Privacy under President Clinton. I conclude that the important thing is to ensure an ongoing privacy policy capability in the executive branch, while a good case can be made for housing it either in the Commerce Department or the Executive Office of the President.

Background on Privacy and the Department of Commerce

Much as is occurring this year, the FTC and Commerce Departments played complementary roles in the mid- to late-1990s in developing privacy policy. At the Federal Trade Commission, privacy initiatives were pushed by Chairman Robert Pitofsky, Commissioners Mozelle Thompson and Christine Varney, and Director of the Consumer Protection Bureau Jodie Bernstein (along with her dedicated staff,

led by David Medine). At the Commerce Department, Barbara Wellbery and Becky Burr played important roles, as did Administrator of the National Telecommunications and Information Administration Larry Irving, General Counsel Andy Pincus, Under Secretary for the International Trade Administration David Aaron, and Secretary William Daley. The history of the FTC's involvement in this period has been well discussed in work by Kenneth Bamberger and Deirdre Mulligan.[3]

The vital work in that period of the Department of Commerce has been less fully discussed.[4] In 1997, Secretary Daley personally hosted a major conference and report on "Privacy and Self-Regulation in the Information Age." That conference engaged many of the persons, and developed many of the concepts, that shaped U.S. privacy policy in the following years.[5] The Department then led the complex and ongoing negotiations with the European Union about how to reconcile the E.U. Data Protection Directive and U.S. law, culminating in the Safe Harbor agreement in 2000, which is still in effect today. For the Safe Harbor and in numerous other privacy issues, the Department, including its International Trade Administration, brought expertise to bear on topics such as E-commerce, international trade, and how privacy fits into broader business practices.

In the summer of 1998, Vice President Gore announced that a privacy policy position would be created in the U.S. Office of Management and Budget. As discussed further below, I entered the role of Chief Counselor for Privacy in early 1999, and worked closely with the Department of Commerce, the FTC, and other agencies until early 2001. Under President George W. Bush, the Commerce Department administered the Safe Harbor program, but did not play as visible a policy role on privacy.

Under President Obama, Secretary Locke created the Internet Policy Task Force , which has published the Green Paper that is the subject of these comments, entitled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework." The Green Paper states:

> "Recommendation #4: Using existing resources, the Commerce Department should establish a Privacy Policy Office (PPO) to serve as a center of commercial data privacy policy expertise. The proposed PPO would have the authority to convene multi-stakeholder discussions of commercial data privacy implementation models, best practices, codes of conduct, and other areas that would benefit from bringing stakeholders together; and it would work in concert with the Executive Office of the President as the Administration's lead on international outreach for commercial data privacy policy. The PPO would be a peer of other Administration offices and components that have data privacy responsibilities; but, because the PPO would focus solely on commercial data privacy, its functions would not overlap with existing Administration offices. Nor would the PPO have any enforcement authority."

For reasons set forth below, I generally support this recommendation, but with greater emphasis on certain functions the Office can play, especially as an ongoing source of institutional expertise on privacy and in order to facilitate the inter-agency clearance of privacy-related issues.

A Complementary Role for a Privacy Office in Commerce -- the Importance of Clearance and International Privacy Issues

To assess the potential usefulness of the PPO, it helps to first understand some important roles played by the Federal Trade Commission in privacy protection:

1. **Enforcement.** The FTC has the power to bring enforcement actions against "unfair and deceptive trade practices," and has negotiated consent decrees on privacy with both large and small companies.
2. **Rulemaking.** In specific areas, such as children's online privacy and anti-spam measures, the FTC has explicit authority to issue rules under the Administrative Procedure Act. More broadly, the FTC could write rules under the more burdensome procedures created by the Magnuson-Moss Act, but it has not chosen to do so on privacy.
3. **Convener.** The FTC has brought together stakeholders in a variety of ways to discuss emerging online privacy issues, and in some instances catalyze industry self-regulatory codes of conduct.
4. **Institutional expertise.** Leading members of today's FTC efforts were also active during the privacy debates of the 1990's. The continuity of FTC staff has contributed to the Commission's institutional expertise on privacy issues.
5. **Bully pulpit.** Top FTC officials and staff direct the attention of companies toward emerging privacy issues.

The Commerce Department has at least two distinctive roles that complement this list of FTC privacy functions: clearance and ability to speak internationally for the Administration.

The role of **"clearance"** is particularly important yet often little understood. In a 2000 document prepared for publication in the Stanford Law Review but not actually published, I went into some detail on the subject.[6] To ensure a unified Administration position, for congressional testimony, Executive Orders, and many other documents, drafts of documents are circulated among the various agencies and components of the Executive Office of the President. Once comments are received, discussions are sometimes needed to resolve differences of opinion, with appeal to more senior officials if differences are not resolved at lower levels. In addition to these structured clearance procedures, agency experts on an issue such as privacy often get engaged earlier in the policy planning process, in a variety of working groups and less-formal methods of sharing expertise and views.

In my experience, an independent agency, such as the FTC, has a sharply limited ability to participate in the Administration's clearance process. On some occasions, a draft document may be shared with the FTC, often early in a policy process, for whatever input the Commission may wish to offer. The decision making, however, is done by persons in the Executive Branch, notably the Executive Office of the President and cabinet agencies such as the Department of Commerce. There are important and long-standing reasons for this separation between independent and executive agencies -- the separation avoids the appearance of political pressure on independent agencies. Separation is especially important for enforcement decisions -- the FTC has true independence on what enforcement

actions it brings, but the corollary is that the FTC is not "inside" the Administration when it comes to creating Administration policy. A variety of rules exist to limit the interaction of independent agencies and the executive branch; new White House officials, for instance, are briefed by counsel to exercise great caution in their interaction with independent agencies.

As an example of the constructive role in clearance played by the Department of Commerce, consider testimony in 2010 on the controversial question of whether and how to amend the Electronic Communication Privacy Act of 1986. ECPA is an important law for law enforcement -- it sets forth the standards by which police and prosecutors can get access to emails and other electronic communications. ECPA, though, is also an important law about corporations and personal privacy. For corporations, ECPA sets the rules for what sorts of access to corporate databases should be permitted, under what circumstances and at what cost. For individuals whose records may be seen by law enforcement, ECPA creates the rules of the road for privacy protection, especially in our modern world when many records are stored in the "cloud" and thus at least potentially accessible to law enforcement.

ECPA thus provides one example of how multiple, compelling values can come into play in clearing the Administration's testimony to Congress. On September 22, 2010, both James Baker of the Department of Justice and Cameron Kerry of the Commerce Department testified before the Senate Judiciary Committee. Under the clearance rules, the testimony of both witnesses had to be shared in advance with the other, and the Administration had to develop a common position. In my experience, sharing a draft document with an agency with a sharply different perspective is often extremely valuable -- assumptions held in the initial agency get challenged, over-statements are modified, and the number of mistakes is reduced. Although I have no direct knowledge of the clearance process in this instance,[7] I think it quite possible that the presence of the Department of Commerce in the process helped create a more nuanced and privacy-protective Administration position.

The ability of an independent agency such as the FTC to have a similar role in clearance is sharply limited. Based on my own experience, and on background discussions with people at the FTC, the FTC is not staffed well enough or situated close enough to the "inside" to engage on the day-to-day clearance of documents on the many law enforcement issues affecting commerce and privacy, including ECPA, the Communications Assistance to Law Enforcement Act, rules about encryption controls, and so forth.

From my time as Chief Counselor for Privacy, the number of privacy issues addressed by federal agencies is far greater than realized by most people who have worked primarily on privacy with the FTC. I offer a list here as an illustration of the sorts of privacy issues that can arise in each of the cabinet departments. For many of the agency activities, there are important implications for commerce, providing a natural role for the Department of Commerce on commercial privacy issues. For others, the link to commerce is less direct, but a broad-based experience with privacy issues at the Department of Commerce will facilitate development of a sound Administration position on privacy:

- Department of Agriculture: migrant worker records.
- Department of Defense and Veterans Affairs: records of service members.
- Department of Education: education records, including for for-profit institutions.
- Department of Energy: smart grid.
- Department of Health and Human Services: medical records; many forms of human services records.
- Department of Homeland Security: numerous issues, including transportation safety and immigration.
- Department of Housing and Urban Development: public housing records.
- Department of Interior: national park reservations and other services provided online.
- Department of Justice: numerous issues.
- Department of Labor: records of union membership.
- Department of State: international privacy issues.
- Department of Transportation: smart roads.
- Department of Treasury: financial privacy; money laundering.

Along with clearance, another role for the executive branch is to **develop and announce the Administration position in international settings.** The Green Paper discusses the Office's role in international privacy activities, but is worth explaining a bit how this would complement any international activities by the FTC.

The FTC plays at least three roles on international privacy issues. First, the FTC is the designated enforcement agency for complaints under the U.S.-E.U. Safe Harbor. Second, the FTC's overall privacy expertise and convening functions inform international discussions about privacy issues, and there has been international cooperation on enforcement actions. Third, last year the FTC for the first time received full member status in the closed session of data protection authorities at the International Conference of Data Protection and Privacy Commissioners. Executive branch officials continue to attend the closed session, as they have since 1999, but with "observer" status.

These important FTC international activities, however, do not replace the need for the executive branch to have policy capability about privacy. For instance, privacy and E-Commerce issues arise in a wide range of bilateral and multilateral trade negotiations -- because transborder data flows are such an important part of modern commerce, data-related issues can arise as one piece of many larger trade negotiations, which often involve the International Trade Administration of the Department of Commerce. Some multilateral fora persistently address privacy issues, such as the Asia-Pacific Economic Cooperation and the Organization for International Cooperation and Development. The U.S. delegations for these activities are led by the executive branch, with representation from the Commerce and State Departments.

More generally, the clearance process applies to developing and implementing the position of the United States in international negotiations. The FTC as an independent agency would have no basis

for making representations, for instance, about what any executive branch agency would accept, including for law enforcement, homeland security, and non-privacy commercial issues. There is thus a sound basis for the Green Paper's recommendation that the Office "would work in concert with the Executive Office of the President as the Administration's lead on international outreach for commercial data privacy policy."

Whether Privacy Policy Should be Centered in the Commerce Department or the Executive Office of the President

I believe there is an extremely strong case in favor of developing an ongoing privacy policy capability in the executive branch. Privacy policy requires familiarity with a complex set of legal, technological, market, and consumer considerations. Good government thus calls for creating an institutional memory and a group of civil servants experienced in privacy policy. This privacy policy capability goes well beyond the need for federal agencies to comply with the Privacy Act and implement good practices for the personal information they hold.

Where to locate this privacy policy capability is less clear. In a 1998 book, Robert Litan and I discussed the question in detail, and concluded that a privacy policy office should be created in the Department of Commerce.[8] From 1999 until early 2001, by contrast, I served in the role of Chief Counselor for Privacy in the U.S. Office of Management and Budget, and I have written reasons for supporting that approach as well.[9]

The chief advantages and disadvantages are mirror-images of each other. Placing the office in the Commerce Department allows for substantially greater staffing, increasing the chance that institutional expertise will accumulate through the ups and downs of public attention to privacy protection. The Commerce Department, however, will be only one of the various agencies who may have views on a particular privacy issue, increasing the risk that privacy will lose out in clearance. On the other hand, placing the policy leadership in OMB or elsewhere in the Executive Office of the President likely improves the possibility of effective coordination of privacy policy across the various agencies. Staffing, however, is always tight at the White House. The Chief Counselor for Privacy, at most, had two full-time staff and one detailee from the Commerce Department.

One model worth considering is the position that Howard Schmidt now fills as Cybersecurity Coordinator. Mr. Schmidt is part of the National Security Staff, and also coordinates with the National Economic Council. My understanding is that a significant amount of support for the Cybersecurity Coordinator is provided by various agencies rather than directly by staff of the Executive Office of the President. A hybrid approach of this sort might achieve more effective privacy policy coordination while also retaining ongoing staffing.

This sort of role might also usefully integrate with the Privacy and Civil Liberties Oversight Board, for which President Obama recently nominated James Dempsey and Elizabeth Collins Cook. That Board, to be effective, should have professional staff to carry out its task of working on privacy and civil

liberties issues that affect anti-terrorist activities. As shown by the example of the Electronic Communications Privacy Act, anti-terrorist and law enforcement activities often have intricate inter-connections with the commercial actors that own and operate most of the infrastructure for processing personal information. It quite possibly makes sense to permit dual tasking of personnel assigned to the Board to work on privacy issues that concern commercial privacy. If this were done, an Executive Office of the President role for a Privacy Coordinator could be supported both by commercial privacy experts and persons assigned to the Oversight Board.

In short, various institutional choices might succeed for institutionalizing privacy policy in the executive branch. The privacy policy capability prior to 2009, and it is a good sign that the Department of Commerce Green Paper is reinvigorating the debate about how best to protect privacy policy while achieving other important goals.

Conclusion

In conclusion, the comments here show important tasks for a Privacy Policy Office in the executive branch, which would complement the FTC's ongoing privacy activities. Notably, such an Office would improve inter-agency clearance, and be important in developing and stating the position of the United States government in international settings. Based on my own discussions with people at the FTC, the FTC does not have the budget or institutional structure to attempt to participate in all of the issues touching on commercial privacy throughout the federal government.

Because these functions complement the existing activities of the FTC, the general effect of such an Office would be to improve privacy policy expertise and capabilities, contrary to the concerns expressed by some privacy advocates that such an Office would undermine privacy protections. In addition to the advantages described above, executive branch participation in development of industry codes of conduct permits expert input from a range of federal agencies and also brings those agencies up to speed on evolving technology. Another advantage is that an executive branch privacy capability can lend force to privacy legislative or other initiatives -- when both the FTC and the Administration work together on an issue, the combined effect is likely to be greater than when an independent agency such as the FTC acts alone. Because the Administration is likely to be asked to provide its views on important legislation in any event, the existence of an ongoing privacy Office in the executive branch will lead to better-informed privacy policy decisions by the Administration.

The existence of such an Office would also provide a more effective structure for the Administration to weigh privacy concerns with other competing policy goals and values. The hope, which I believe is supported by experience, is that participation by privacy experts in executive branch decisions increases the likelihood of win-win situations, in which privacy goals are better achieved and other goals as well.

In short, the Department of Commerce deserves praise for advancing the idea of an ongoing Privacy Policy Office as part of its Green Paper.

[1] Peter Swire is the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University, and a Senior Fellow at the Center of American Progress. From 1999 through early 2001 he served as Chief Counselor for Privacy in the U.S. Office of Management and Budget. From 2009 through August, 2010 he served as Special Assistant to the President for Economic Policy, including on privacy and related technology issues.

[2] Juliana Gruenwald, "Privacy Groups Critical of Commerce Privacy Report," National Journal, Dec. 16, 2010, available at http://insidegoogle.com/2010/12/privacy-groups-critical-of-commerce-privacy-report/.

[3] See Kenneth Bamberger & Deirdre Mulligan, "Privacy on the Books and on the Ground," forthcoming Stanford Law Review, available at http://ssrn.com/abstract=1568385; Kenneth Bamberger & Deirdre Mulligan, "Catalyzing Privacy: New Governance, Information Practices, and the Business Organization," forthcoming Law & Policy, available at http://ssrn.com/abstract=1701087. I have written previously on the history of the late 1990s in privacy regulation. Peter P. Swire, "Trustwrap: The Importance of Legal Rules to Internet Privacy and E-Commerce," 54 Hastings L.J. 847 (2003), available at http://ssrn.com/abstract=424167.

[4] One reason may be the untimely death in 2003 of Barbara Wellbery, who worked tirelessly to address the issues of U.S. and E.U. relations in connection with the European Union Data Protection Directive and was instrumental to creation of the Safe Harbor privacy program that is now administered by the Department of Commerce.

[5] The conference invitation pushed me to write "Markets, Self-regulation, and Government Enforcement in the Protection of Personal Information," my first article specifically on privacy issues.

[6] Peter P. Swire, "The Administration Response to the Challenges of Protecting Privacy," (Jan. 8, 2000 unpublished draft), available at http://www.peterswire.net/stanford7.doc.

[7] I served in the National Economic Council until August, 2010, before the September, 2010 testimony described in the text.

[8] Peter P. Swire & Robert E. Litan, None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive (Brookings, 1998), at 179-188.

[9] Peter P. Swire, "The Administration Response to the Challenges of Protecting Privacy," (Jan. 8, 2000 unpublished draft), available at http://www.peterswire.net/stanford7.doc.