

Q&A: Advice to the next Homeland Security CPO

Jay Cline

January 26, 2009 ([Computerworld](#))

*If you had a chance to pose any question to the person in charge of protecting Americans' privacy as the [U.S. Department of Homeland Security](#) executes its mission, what would you say? I had that chance this month when **Hugo Teufel**, departing chief privacy officer at the DHS, delivered an address, entitled "Reflections on My Time as DHS CPO of the War on Terror," to the [Twin Cities Privacy Retreat](#).*

After the address, I cornered Teufel for some follow-up questions. Those and his answers follow.

Your last public act as DHS CPO was to release a report ([download PDF](#)) critical of data practices at European hotels. What do you hope this will accomplish? Critical of hotels? No. We issued a report that set forth the facts and the law, as we currently understand them, about data protection in the "third pillar" and in certain [EU](#) member states with regard to security service collection and use of hotel guest registration data, a common practice throughout Europe. If we were critical, it was of the officials who were reluctant in being transparent about what their security services do with hotel guest registration data.

In your speech, you said U.S. CPOs would be wise to understand how the [European Union treats privacy](#) differently within its "first pillar" commercial policy and "third pillar" security areas. Can you elaborate? The rules covering the same personally identifiable information appear to be different for security services than they are for businesses operating in the EU. Security services may make demands of businesses for certain data, which by law the businesses are not allowed to collect. The businesses can refuse, risking the wrath of the security service, or they can comply, risking punishment from the data-protection authority, which may

not have competence over the security service collection and use of that data. It's a real catch-22.

What was your top lesson learned from the U.S.-EU compromise on the sharing of airline passenger name records? Sadly, that politics sometimes took precedence over the security and privacy of Americans and Europeans.

Any takeaways from the U.S.-EU dispute over [U.S. government access to SWIFT data](#)? Hey, that involved Treasury, not DHS! I will say that, generally speaking, one should be on firm legal and policy footing when trans-Atlantic data flows are concerned. Certainly, never underestimate the importance of data protection to the Europeans.

You mentioned that you put a lot of materials on the [DHS privacy Web site](#). What do you wish the public knew more about regarding DHS's privacy function? I wish the public knew how hard we work to protect their privacy while the department secures the homeland. We are at the forefront of American privacy protection domestically and internationally. Come visit our Web site, and you will see what I mean.

You have 35 people on staff. What do they do? A lot! Our compliance team is responsible for all privacy impact assessments and system-of-records notices at the department. Our technology and intelligence team handles the thorny issues involving the interface between privacy and technology and intelligence community activities. Our privacy incidents and inquiries team investigates incidents and complaints. Our international privacy policy team stays abreast of the latest developments with the EU, APEC [Asia-Pacific Economic Cooperation], ISO and various other international and multinational organizations. On the [Freedom of Information Act] side, our office sets FOIA policy for the department and handles requests for many of the department-level components. Finally, our director of administration keeps it all running.

After you read my recent *Computerworld.com* column "[What Trumps Privacy?](#)" we spoke, and you mentioned that there has been an ongoing debate inside your office over the meaning of privacy. Care

to elaborate? We [in the office] have had an ongoing, occasional discussion over what privacy is. Is it a fundamental right, a liberty interest or a social construct? If it is a fundamental right, why then are there such wide differences in the way we and the Europeans approach privacy? Most Americans would reject [national identification cards](#) and the widespread European practice of registering with the police where one lives. The Europeans, who pride themselves for recognizing the fundamental right of privacy, widely accept these practices and other security service actions that most Americans would find odious. By the way, the current consensus in the office is that privacy embodies aspects of all three categories.

Have privacy advocates helped flag anything for you regarding DHS operations that pushed the privacy envelope? We interact regularly with the privacy advocacy community and have sought out their thoughts and guidance on new systems and technologies. We're often on the same track as they are on what the salient privacy issues are. The advocacy community plays an important role in privacy protection, and we acknowledge it.

Can you point to any government program that has been shut down because it lost public credibility over its privacy practices? At DHS? No. There are two programs, however, that bear mentioning: Fidnet and Talon. Fidnet -- Federal Intrusion Detection Network -- was a Clinton-era effort led by [Richard Clarke](#) to put in place comprehensive cybersecurity measures for the whole nation. The failure to consider privacy and civil liberties issues led to Fidnet's significant downscaling and the loss of several years before the federal government again took up a comprehensive cybersecurity program. Talon -- Threat and Local Observation Notice -- was a force-protection system designed by the Air Force but taken over by the Pentagon's Counter Intelligence Field Activity. The failure to properly educate and train persons reporting into Talon led to violations of the Privacy Act and shutting down of the program.

In your speech, you said, "If you stick to the [fair information principles](#), you'll always come out with the right answer." What do

you think is the most important principle when it comes to privacy in the war on terror? Hands down, the most important principle is transparency. Congress often makes key decisions on programs, and agencies have to implement them. Transparency lets the public understand the implications of those decisions and shows the public how well the agency has built in privacy, whether or not Congress considered the privacy implications when it passed the legislation.

What is the hardest thing about the DHS CPO job? Having to say good-bye at the end of my term.

What did your predecessor, Nuala O'Connor Kelly, do well? Three things. First, she hired the best privacy professionals in the public sector. Second, she set up the office with compliance, technology and international privacy policy functions, and a senior policy adviser to handle complex matters. Third, she relentlessly extolled the office and the position in her outreach efforts, often overseas.

What's left to do for your successor? Much. Finishing the FOIA/Privacy Act regulations. I couldn't get them across the finish line, although we made great progress on them. Providing policy advice to senior leaders is never-ending. To do that, my successor is going to have to get to know the key players in the department, career and appointed, and learn about all of the things that the department does is another. I had a real advantage by being at the department for over two and a half years before joining the Privacy Office.

Any advice for your successor? Know who you work for. Know who your stakeholders are. Understand the differences between the two. Either can kill you, but for different reasons. Also, remember that you can be inside the organization or outside the organization, but you can't be both. Above all, never forget what the mission is, for the department and for the office.

All told, I think the record has to show two things for Teufel and his predecessor, O'Connor Kelly: The [Department of Homeland Security](#) has not become Big Brother, and the DHS's ability to prevent another terrorist attack on U.S. soil has not been unduly curtailed by extreme views of

privacy. Whether [President Obama](#) appoints another CPO in this mold of principled pragmatism may be one of his most important subcabinet decisions.

Jay Cline is a former chief privacy officer at a Fortune 500 company and is now president of [Minnesota Privacy Consultants](#). You can reach him at cwprivacy@computerworld.com.