Catholic University Journal of Law and Technology

Volume 25 | Issue 1 Article 1

2017

Thriving in the Online Environment: Creating Structures to Promote Technology and Civil Liberties

Daniel W. Sutherland
U.S. Department of Homeland Security

THRIVING IN THE ONLINE ENVIRONMENT: CREATING STRUCTURES TO PROMOTE TECHNOLOGY AND CIVIL LIBERTIES

Daniel W. Sutherland[1]

The online environment is dramatically impacting our world. A global research organization has concluded that there are now more mobile devices in the world than there are people, and that these devices are multiplying five times faster than the human population.[2] In *Riley v. California*, Chief Justice John Roberts observed that "modern cell phones . . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[3] One commentator rightly observed that the "Internet . . . . has become the backbone to the 21rst Century infrastructure[.]"[4] IBM CEO Ginni Rometty has said that data "is the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry."[5] It is commonly estimated that ninety percent of all the data in the world has been generated in the past three years.[6] This new age is bringing

1 Daniel W. Sutherland is the Associate General Counsel for the National Protection and Programs Legal Division within the Department of Homeland Security's Office of the General Counsel. From 2003 to 2009, he was the Department's Officer for Civil Rights and Civil Liberties. The views expressed in this article do not represent the Department of Homeland Security and are entirely those of the author. This article is based on Mr. Sutherland's remarks at the Catholic University Journal of Law and Technology Symposium, Cybersecurity and Privacy in the Internet Economy: Information Sharing, Data Security, and Intellectual Property," March 1, 2016.

2 Zachary Davies Boren, *There Are Officially More Mobile Devices Than People in The World*, THE INDEPENDENT, (Oct. 7, 2014), http://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html.

3 Riley v. California, 134 S.Ct. 2473, 2484 (2014).

4 Dan Perrin, *Cyber education is necessary for the future of mankind*, WASH. EXAMINER (Sept. 5, 2016, 12:04 AM), http://www.washingtonexaminer.com/cyber-education-is-necessary-for-the-future-of-mankind/article/2600936.

5 Ginni Rometty, Chairman, President & CEO, IBM, IBM Security Summit: New Ways of Thinking about Enterprise Security (May 14, 2015).

6 *Big Data: For better or worse: 90% of world's data generated over last two years,*

concrete changes to our economic activities, to how we learn, to our enjoyment of sports and music, and to our understanding and practice of religion.

However, there are potential risks that must be addressed. The security of the data that is now online is one such risk. How this explosion of data impacts our civil rights, civil liberties and privacy is another. Now foreign governments and private sector entities have access to treasure troves of data about our movements through the day, the books we read and the people we associate with. As information is becoming the new coin of the realm, the appropriate uses of that information are becoming, and will remain, a core issue. In an online environment, civil rights, civil liberties and privacy are not a niche issue to be considered, but become a fundamental matter that must be addressed.

One method for addressing civil rights, civil liberties and privacy challenges is to create structures that will help our institutions of government and commerce to better understand these issues and devise strategies to address them. In fact, government and private sector entities are creating such structures – organizations that work on the inside, that are welcomed as colleagues, that identify issues at an early stage, and that give advice on how to design programs and capabilities in ways that enhance privacy, civil rights and civil liberties. These structures can help build the public's confidence that the government and corporations can be trusted to handle data with discretion and effectiveness. This article will describe two organizations within the U.S. Department of Homeland Security that have had a valuable impact on the way that security policies are being crafted. It will also identify other similar organizations in the public and private sectors. Finally, it will examine a case study – a cybersecurity capability that has been dramatically influenced by the inclusion of privacy and civil liberties professionals from the outset.

STRUCTURES FOR ENHANCING CIVIL RIGHTS AND CIVIL LIBERTIES IN THE DEPARTMENT OF HOMELAND SECURITY

A. Overview of the Homeland Security Act

In 2003, the President signed the Homeland Security Act. The new law brought together twenty-two federal agencies and over 180,000 employees with the mission of guarding the nation's borders, enhancing the security of America's airports, and helping build resilience of the country's infrastructure.[7] The Homeland Security Act also included several innovative steps, including

---

SCIENCE DAILY (May 22, 2013), https://www.sciencedaily.com/releases/2013/05/130522085217.htm

[7] Homeland Security Act of 2002, 6 U.S.C. §§ 2-230 (2012).

the creation of two positions dedicated solely to the protection of civil rights and civil liberties. The Congress thereby created a unique model of decision-making: for the first time in the federal government, an agency has two members of the senior leadership, reporting directly to the Cabinet Secretary, to focus solely on how the agency's decisions impact individual liberties.

B. The Officer for Civil Rights and Civil Liberties

The Homeland Security Act required that the President appoint an Officer for Civil Rights and Civil Liberties to "assist the Secretary in the performance of the Secretary's functions[.]"[8] Section 705 of the Homeland Security Act gives the Officer several tasks. The first is an investigative function – when a citizen has a civil rights-related complaint, the Officer shall "review and assess information concerning abuses of civil rights, civil liberties, and profiling on the basis of race, ethnicity, or religion, by employees and officials of the Department . . . ."[9] The second task is to develop and shape policy wherein the Officer shall "assist the Secretary, directorates, and offices of the Department to develop, implement, and periodically review Department policies and procedures to ensure that the protection of civil rights and civil liberties is appropriately incorporated into Department programs and activities. . . ."[10] The third major task is a compliance function – to review programs to ensure the Department's actions are in accordance with "constitutional, statutory, regulatory, policy, and other requirements related to the civil rights and civil liberties of individuals affected by the programs and activities of the Department. . . ."[11] In all its work, the Officer is required to coordinate with the Department's Privacy Officer.[12]

Thus, Congress created a unique civil rights office.[13] While other federal agencies had offices that focus on civil rights, this was the only office that included "and Civil Liberties" in the title.[14] The title shows that the Office addresses issues at the intersection of national security, civil rights, and civil lib-

---

8 *Id*. at § 103(d) (2012).
9 *Id*. at § 705(a)(1) (2012).
10 *Id*. at § 705(a)(3) (2012).
11 *Id*. at § 705(a)(4) (2012).
12 *Id*. at § 705(a)(5) (2012).
13 DEP'T OF HOMELAND SEC.: OFF. FOR C.R. & C.L., REPORT TO CONGRESS ON IMPLEMENTATION OF SECTION 705 OF THE HOMELAND SECURITY ACT & THE ESTABLISHMENT OF THE OFFICE FOR CIVIL RIGHTS & CIVIL LIBERTIES 12 (2004), https://www.dhs.gov/xlibrary/assets/CRCL-ReportJun04.pdf [hereinafter DHS REPORT TO CONG.].
14 Daniel W. Sutherland, Officer for Civil Rights & Civil Liberties, DHS, Homeland Security Office for Civil Rights and Civil Liberties: A One-Year Review (July 1, 2004).

erties.[15] Moreover, the Office has a distinctive internal function – assisting the senior leadership to develop policies and initiatives in ways that protect civil rights and civil liberties. The Office also has the simultaneous function of providing compliance reviews and investigations of complaints. Finally, the Office also has the responsibility for overseeing the Department's equal employment opportunity program.[16] This brings all civil rights-related issues under one office, including those with regard to the Department's own employees and those with regard to how the Department's programs impact the general public.[17]

Substantial investment has been made in this function. Secretary Thomas Ridge[18] decided that the Officer would be part of the senior leadership of the Department, reporting directly to him, and the Congress later codified that decision.[19] Moreover, the Department has committed substantial resources to the Office.[20] The Office's budget is $21.8 million, which funds approximately 90 employees and several substantial programs.[21] The Congress and the Department have been so pleased with the contributions of the Office for Civil Rights and Civil Liberties that they have expanded its role (adding several new provisions into the authorizing language in Section 705 of the Homeland Security Act) and its budget (moving from a staff of approximately 40 in 2004 to a staff of almost 100 currently).[22]

The Office for Civil Rights and Civil Liberties makes its contributions in several areas. One of the key elements of Office's mission is to provide proactive advice to the senior leadership of the Department.[23] In its most recent Annual Report to Congress, the Office states its first mission as, "[p]romoting respect for civil rights and civil liberties in policy creation and implementation by advising Department leadership and personnel, and state and local partners."[24] The Office has had broad impact across the Department, including

---

15 DHS REPORT TO CONG., *supra* note 13.

16 *Id.*

17 *Id.*

18 *Thomas J. Ridge, Homeland Security Secretary 2003-2005*, DHS, https://www.dhs.gov/thomas-j-ridge (last updated May 16, 2016).

19 Homeland Security Act of 2002, 6 U.S.C. § 704 (2012); *see also* DEP'T OF HOMELAND SEC.: OFF. FOR C.R. & C.L., FISCAL YEAR 2015 ANNUAL REPORT TO CONGRESS 6 (2016), https://www.dhs.gov/sites/default/files/publications/crcl-fy-2015-annual-report.pdf [hereinafter DHS 2015 FISCAL REPORT].

20 DHS 2015 FISCAL REPORT, *supra* note 19.

21 *Id.*

22 *Cf.* Report to Congress on Implementation of Section 705 of the Homeland Security Act and the Establishment of the Office for Civil Rights and Civil Liberties (June 2004); *see also* DHS 2015 FISCAL REPORT at iv.

23 DHS 2015 FISCAL REPORT at 11.

24 *Id.* at 5.

shaping new screening protocols at airports, improving immigration processes, building civil liberties protections into cybersecurity policies, enhancing intelligence analysis, and improving conditions in detention facilities.[25]

Two examples illustrate the Office's impact on policy. In the first months of the new Department, the Office was an integral part of the Department's review of the Department of Justice, Office of Inspector General report on the treatment of aliens detained in connection with the September 11th terrorism investigations.[26] As a result of that work, the Department sent guidance to all immigration officers directing that detainees be given notice of the charges against them within 72 hours of the time they are detained; established new detention standards to improve communications between detainees and immigration officials, allowing for more oversight of conditions; and, established a policy that immigration officers make an individualized and independent decision on bond and the closing of hearings every time an individual is detained. [27]

A second example is in the technology area; the Office helped to create an innovative program to provide accessible technology to people with disabilities.[28] Section 508 of the Rehabilitation Act of 1973, as amended, requires the federal government to ensure that electronic and information technology is accessible to persons with disabilities.[29] The law applies to all federal agencies as they develop, procure, maintain or use such technologies.[30] This includes products and services such as computer hardware and software, telecommunications products, information kiosks, and web sites. Therefore, the Office for Civil Rights and Civil Liberties co-chaired a project with the Chief Information Officer to create the Office of Accessible Systems and Technology (OAST).[31] The purpose of this office is to "ensure that all electronic information and technology procured, developed, maintained, or used is accessible to DHS employees and customers with disabilities through a range of policy, training, technical assistance and compliance activities."[32] This innovative function has had enormous impact, including testing hundreds of IT and web-based apps, remediating tens of thousands of pages of inaccessible documents posted on the DHS websites, creating an Accessibility Compliance Center of Excellence, administering a robust training program, and creating a Department-wide helpdesk for accessibility questions.[33] The office has also emerged as a recog-

---

25 *Id.* at 7-8.
26 DHS REPORT TO CONG., *supra* note 13, at 18.
27 *Id.* at 19.
28 *Id.* at 21.
29 Rehabilitation Act of 1973, 29 U.S.C. § 794(d) (2012); DHS REPORT TO CONG., *supra* note 13, at 21.
30 DHS REPORT TO CONG., *supra* note 13, at 21.
31 DHS 2015 FISCAL REPORT, *supra* note 19, at 57.
32 *Id.* at 7-8.
33 *Id.* at 58.

nized leader across government; for example, it has in recent years helped lead a cross-government effort to develop a "trusted tester" program.[34]

In addition to proactive policy advice and development, the Office has focused on areas such as training. It created the "Civil Rights and Civil Liberties Institute" to provide training on a large scale to the Department's large workforce.[35] In the first year of the Department's existence, the Office became responsible for training law enforcement officers on the government's policy against racial profiling.[36] It has provided training to Department employees on a wide range of additional issues, such as screening involving religious travelers, and has worked with the Federal Law Enforcement Training Center to enhance its training on Constitutional law.[37]

The Office also contributes by convening forums for members of the public communicate with homeland security leaders.[38] The Office has created regular community roundtables in 16 cities across the country and periodic meetings in other locations.[39] There are two purposes for these roundtables: to enable citizens to communicate their concerns directly with homeland security officials, and to explain the Department's policies to citizens.[40] These roundtables have significantly benefited Department leadership as they receive direct feedback on how programs and operations are being received, and then incorporate the best ideas into new policy initiatives. This then produces greater trust between communities and homeland security officials.[41]

Finally, the Office has made an impact on the Department through its role in investigating and resolving complaints from the public that the Department has in some way violated civil rights or civil liberties.[42] This internal audit function is incredibly valuable to the Department's leadership.[43] First, it provides early warning signs of potential abuses. Second, it allows them the opportunity to resolve issues at an early stage, often before problems become the subject of litigation, Congressional oversight or public outcry. Finally, it promotes public

---

34 *Id*.

35 *Id*. at 11.

36 *See Civil Rights and Civil Liberties Institute*, DHS.GOV, https://www.dhs.gov/civil-rights-and-civil-liberties-institute, (last visited Oct. 7, 2016); see also DHS 2015 FISCAL REPORT, *supra* note 19, at 16.

37 *Civil Rights and Civil Liberties Institute*, DHS.GOV, https://www.dhs.gov/civil-rights-and-civil-liberties-institute, (last visited Oct. 7, 2016).

38 DEP'T OF HOMELAND SEC.: OFF. FOR C.R. & C.L., FISCAL YEAR 2014 ANNUAL REPORT TO CONGRESS 11 (2016), https://www.dhs.gov/sites/default/files/publications/crcl-fy-2014-annual-report_0.pdf [hereinafter DHS 2014 FISCAL REPORT].

39 *Id*. at 13.

40 *Id*. at 11-12.

41 DHS 2015 FISCAL REPORT, *supra* note 19, at 13-14.

42 *Id*. at 27.

43 Sutherland, *supra* note 14.

confidence because of the credibility of these investigations – the Office demonstrates to stakeholders that these investigations do result in concrete improvements undertaken by the Department.

C. The Chief Privacy Officer

The Homeland Security Act required that the Secretary appoint a Chief Privacy Officer. Section 222 of the Act provides that the Chief Privacy Officer reports directly to the Secretary of Homeland Security.[44] Thus Congress established "the first statutorily required comprehensive privacy operation at any federal agency."[45] Then-Secretary Ridge stated that the Privacy Office "will be involved from the very beginning with every policy initiative and every program initiative that we consider, to ensure that our strategy and our actions are consistent with not only the federal privacy safeguards already on the books but also with the individual rights and civil liberties protected by the Constitution."[46]

The Privacy Office's scope and influence is not limited to the Department's headquarters; it is enhanced by parallel privacy offices in components such as FEMA and the National Protection and Programs Directorate.[47] The Chief Privacy Officer's responsibilities fall into several categories. First, the CPO is responsible for privacy policy within the Department, which, under Section 222(b), includes:

> assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection and disclosure of personal information; . . . .
>
> evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;
>
> conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected;
>
> coordinating with the Officer for Civil Rights and Civil Liberties to ensure that –
>
> programs, policies, and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner; and,
>
> Congress receives appropriate reports on such programs, policies, and procedures; and
>
> preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of

---

44 Homeland Security Act of 2002, 6 U.S.C. § 142(a) (2012).

45 U.S. DEP'T OF HOMELAND SEC.: PRIVACY OFF., ANN. REP. TO CONGRESS 1 (2003-2004), https://www.dhs.gov/sites/default/files/publications/privacy_annualrpt_2004.pdf [hereinafter PRIVACY OFF. 2003-04 REPORT TO CONG.].

46 *Id*.

47 Nuala O'Conner Kelly, Chief Privacy Officer, U.S. Dep't of Homeland Sec., Keynote Address at the 25th International Conference of Data Protection Privacy Commissioners (Sept. 11, 2003).

the Privacy Act of 1974, internal controls, and other matters.[48]

One example of how the Department has leveraged the expertise of privacy professionals has been in developing policies and protocols with the European Union.[49] From the beginning of the Department's existence the Privacy Office has worked closely with the Europeans on issues related to "passenger name record" data – information about people who are planning to fly to the United States.[50] The office played a key role in advising the Department on the issues involved in obtaining this information.[51] After the United States entered into an agreement with the European Union in 2004, the Privacy Office then took on an important role in implementing the terms of the "Passenger Name Record" (PNR) agreement. For example, it posted "privacy statements that might be used by airlines, travel industry representatives, and central reservation systems."[52] The office was also responsible for annual joint reviews of the implementation of the PNR Agreement, a key aspect of ensuring credibility with the European authorities.[53] These responsibilities associated with the PNR agreement continue, with the office in 2015 undertaking a Privacy Compliance Review of the Department's implementation of the 2011 version of the PNR agreement.[54]

Other examples of leveraging the expertise of the Privacy Office includes involvement with evaluating policy on unmanned aerial vehicles,[55] reviewing the operations of all fusion centers around the country,[56] and helping to shape the Department's approach to "big data."[57] The Privacy Office invests a great deal in reviewing Department programs and operations to determine how those

---

48 6 U.S.C. § 142.

49 PRIVACY OFF. 2003-04 REPORT TO CONG., *supra* note 45, at 11.

50 U.S. DEP'T OF HOMELAND SEC.: PRIVACY OFF., A REP. CONCERNING PASSENGER NAME REC. INFO. DERIVED FROM FLIGHTS BETWEEN THE U.S. AND THE E.U. 2 (2008), https://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf [hereinafter PASSENGER NAMES].

51 PRIVACY OFF. 2003-04 REPORT TO CONG., *supra* note 45, at 14.

52 *Id*.

53 *Id*.

54 U.S. DEP'T OF HOMELAND SEC. PRIVACY OFF., ANN. REP. TO CONGRESS 3 (2014-2015), https://www.dhs.gov/sites/default/files/publications/dhsprivacyoffice2015annualreport-final-11102015.pdf [hereinafter PRIVACY OFF. 2014-15 REPORT TO CONG.].

55 U.S. DEP'T OF HOMELAND SEC. PRIVACY OFF., FINAL ANN. REP. TO CONGRESS 2 (2014), https://www.dhs.gov/sites/default/files/publications/dhs-privacy-office-2014-annual-report-FINAL.pdf [hereinafter FINAL 2014 ANN. REPORT TO CONG.].

56 U.S. DEP'T OF HOMELAND SEC. PRIVACY OFF., ANN. REP. TO CONGRESS ii (2009-2010), https://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2010.pdf [hereinafter PRIVACY OFF. 2009-10 REPORT TO CONG.].

57 FINAL 2014 ANN. REPORT TO CONG., *supra* note 55, at 2.

initiatives measure up against federal privacy protection statutes[58] and Departmental policy.[59] The Office's compliance work "ensures that privacy protections are built into Department systems, initiatives, projects, and programs as they are developed and modified."[60] The Office uses tools such as Privacy Threshold Analyses, Privacy Impact Assessments (PIAs), and Privacy Compliance Reviews.[61] These tools help to integrate compliance process into the Department's daily work and its rhythm of developing, deploying, and reviewing programs. By engaging with program managers at the earliest stages of program design, the Privacy Office is able to ensure that Fair Information Practice Principles are understood and considered in the development stage.[62] In fiscal year 2015 alone, the Office participated in the development of 47 new or updated PIAs and published 27 Systems of Records Notices.[63]

This compliance work has dramatically impacted the Department's cybersecurity mission. The DHS website posts PIAs related to major cybersecurity programs (and also has several other PIAs on other cyber programs that are now retired).[64] For example, privacy professionals have carefully examined all three generations of the EINSTEIN intrusion detection and prevention capability and issued extensive PIAs on the programs.[65] The PIAs document how the programs have been improved through the application of privacy principles, and enhance public trust and confidence because of the transparency of these reviews.[66]

---

58 *See* Authorities and Responsibilities of the Chief Privacy Officer, available at https://www.dhs.gov/chief-privacy-officers-authorities-and-responsibilities, citing the Privacy Act of 1974, the E-Government Act of 2002, the Freedom of Information Act of 1966, and the Implementing the Recommendations of the 9/11 Commission Act of 2007.

59 *Privacy Office*, DHS.GOV, https://www.dhs.gov/privacy-office (last updated July 28, 2016).

60 PRIVACY OFF. 2014-15 REPORT TO CONG., *supra* note 54, at 30.

61 *Privacy Compliance*, DHS.GOV, https://www.dhs.gov/compliance (last updated June 10, 2016); *Privacy Impact Assessments*, DHS.GOV, https://www.dhs.gov/privacy-impact-assessments (last updated Aug. 24, 2015); *Privacy Reviews and Investigations*, DHS.GOV. https://www.dhs.gov/investigations-reviews (last updated June 17, 2016).

62 PRIVACY OFF. 2014-15 REPORT TO CONG., *supra* note 54, at 30.

63 *Id.* at 2.

64 *Cybersecurity and Privacy*, DHS.GOV, https://www.dhs.gov/cybersecurity-and-privacy (last visited Oct. 6, 2016). Privacy Impact Assessments have been posted on all three generations of the EINSTEIN intrusion detection program, the Enhanced Cybersecurity Services program, and the National Cybersecurity Protection System. See https://www.dhs.gov/privacy-documents-national-protection-and-programs-directorate-nppd.

65 *See Einstein*, DHS.GOV, https://www.dhs.gov/einstein (last visited Oct. 6, 2016) ("The Department of Homeland Security (DHS) has the mission to provide a common baseline of security across the federal executive branch . . . this common baseline is provided in part through the EINSTEIN system.").

66 *Privacy Documents for the National Protection and Programs Directorate (NPPD)*, DHS.GOV, https://www.dhs.gov/privacy-documents-national-protection-and-programs-

The Office has broad impact across the Department through its extensive training programs. The Office leads both in-person and web-based training programs, reaching thousands of employees every year through efforts such as new employee training, the "Compliance Boot Camp," and training for fusion centers.[67] Just as with the Office for Civil Rights and Civil Liberties, the Privacy Office provides forums for the Department's leadership to engage with interested stakeholders. It has established a formal advisory board, the Data Privacy and Integrity Advisory Committee, which meets regularly to study DHS programs and operations, provide feedback to the Department, and issue recommendations for improvements.[68] Finally, the Privacy Office is also responsible for programmatic functions such as leading the Freedom of Information Act program for the Department and administering the obligations in the Privacy Act.[69]

The Chief Privacy Officer's responsibilities are broad and designed to ensure that the influence of privacy professionals will be felt in all corners of the Department's programs and operations. Over the Department's twelve years, privacy professionals have substantially impacted and improved the Department's programs and operations.

D. Exporting the Model

The Department of Homeland Security stands out because it has two civil libertarians in senior leadership – their sole motivation being protecting privacy, civil rights and civil liberties.[70] These officers provide preventative advice and serve as internal auditors, investigating concerns and ensuring compliance in such a credible way that it builds public trust and confidence. These officers have been given substantial resources, and have reach across the entire Department.[71]

The success of the Homeland Security Office for Civil Rights and Civil Liberties has led Congress and the Executive Branch to mandate similar offices across the Executive Branch.[72] In 2007, Congress passed the Implementing Recommendations of the 9/11 Commission Act, which required enhanced

---

directorate-nppd (last visited Oct. 6, 2016).

67 PRIVACY OFF. 2014-15 REPORT TO CONG., *supra* note 54, at 25.

68 *Id.* at 20.

69 *Id.* at 9, 20.

70 Daniel W. Sutherland, *Security and Freedom: Honoring our Values*, DHS.GOV (Dec. 17, 2007), https://www.dhs.gov/journal/leadership/2007/12/security-and-freedom-honoring-our.html.

71 *Civil Rights and Civil Liberties*, DHS.GOV (Oct. 5, 2015), https://www.dhs.gov/topic/civil-rights-and-civil-liberties.

72 Civil Rights Act of 1964, 42 U.S.C. § 2000ee-1 (2014).

screening of cargo entering the country, redistributed counter-terrorism funding, and authorized fusion centers.[73] One of most significant provisions of the law was to require Cabinet agencies to "designate not less than 1 senior officer to serve as the principal advisor to" assist the agency in developing policies and programs in ways that comport with civil rights and civil liberties.[74] Congress thus required that the Departments of Justice, Defense, Treasury, Health and Human Services, and Homeland Security, along with the Central Intelligence Agency (CIA), and the Office of the Director of National Intelligence (ODNI), have a privacy and civil liberties office. The responsibilities for these offices are modeled on the authorities given to DHS's Office for Civil Rights and Civil Liberties and Chief Privacy Office:

> "assist the head of such department … in appropriately considering privacy and civil liberties concerns when such officials are proposing, developing, or implementing laws, regulations, policies, procedures, or guidelines;"
>
> conduct reviews of "department … actions, policies, procedures, guidelines, and related laws and their implementation to ensure that such department … is adequately considering privacy and civil liberties in its actions;" and,
>
> ensure that the department has "adequate procedures to receive, investigate, respond to, and redress complaints from individuals[.]"[75]

Congress provided principals to guide their work:

> "that the need for power is balanced with the need to protect privacy and civil liberties;"
>
> "that there is adequate supervision of the use by such department, agency, or element of the power to ensure protection of privacy and civil liberties; and,
>
> "that there are adequate guidelines and oversight to properly confine its use."[76]

Therefore, other Cabinet departments now have the ability to benefit from structures similar to those that have been in place at DHS since 2003. The Cabinet departments and the Congress are making decisions on how to fund each office and how to place the offices in the agencies' organizational structure. While the departments are deciding daily how to integrate these offices into the daily operations of the agency, the structures are in place.

These civil liberties entities could benefit a wider range of government agencies and many private companies. For example, consider if a major urban police department appoints a senior advisor to the chief of police who is focused on civil rights and civil liberties. If this senior advisor was given a substantial staff and resources, the police department would quickly benefit from improvements in training, in better policies and protocols governing SWAT teams, in policies for responding to crowd disturbances, and in engaging with

---

73 Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2007).

74 *Id*.

75 42 U.S.C.A. § 2000ee-1 (2014).

76 42 U.S.C.A. § 2000ee-1(a)(1)-(3) (2014).

the community. Similarly, a company that collects information about consumers could build confidence and trust among its customers and regulators if it has a privacy office with resources and influence inside the organization.

CASE STUDY: AUTOMATED INDICATOR SHARING

Privacy and civil liberties professionals within the Department of Homeland Security have been able to strongly influence the development of policy and the tactical daily operations of programs. The Department's cybersecurity program offers a recent example of the impact privacy and civil liberties professionals can have.

A. The Foundation for Information Sharing

Cybersecurity has emerged as one of the country's top national security threats.[77] The Administration and Congress have therefore decided that the country must have "an ecosystem where as soon as a company or federal agency observes an attempted compromise, the indicator will be shared in real time with all of our partners, protecting them from that particular threat.[78] That means adversaries can only use an attack once, which increases their costs and ultimately reduces the prevalence of cyber attacks."[79]

Any analysis of the Cybersecurity Act of 2015 must begin one year earlier, with the passage of the National Cybersecurity Protection Act of 2014 (NCPA).[80] This law codified the role of DHS's National Cybersecurity and Communication Integration Center (NCCIC), and laid the foundation for the future legislation.[81] The NCPA establishes the NCCIC as a central player in the federal government's information sharing about cybersecurity risks with the private sector, as well as an entity that provides cybersecurity technical assistance and incident-response capabilities to the private sector upon request.[82] Moreover, the NCPA authorizes the NCCIC to develop and regularly exercise cyber incident response plans. The NCPA makes clear that the

---

77 Sandra I. Erwin, Stew Magnuson, & Jasmin Tadjdeh, *Top Five Threats to National Security in the Coming Decade*, NAT'L DEF. INDUS. ASS'N (Nov. 2012), http://www.nationaldefensemagazine.org/archive/2012/november/pages/topfivethreatstonationalsecurityinthecomingdecade.aspx.

78 *Automated Indicator Sharing*, DHS.GOV, https://www.dhs.gov/ais# (last visited Oct. 17, 2016).

79 *Id.*

80 National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066 (2014).

81 *Id.*

82 *Id.*

NCCIC's information sharing and technical assistance authorities are not explicitly limited to critical infrastructure but rather apply more broadly to federal and non-federal entities.[83] Almost exactly one year later, the President signed the Cybersecurity Act of 2015.[84]

B. The Cybersecurity Act of 2015

Background

As a result of the 2014 NCPA, and under the authority of Presidential Policy Directive 21, the Department of Homeland Security began developing a capability that would allow machine-to-machine sharing of cyber threat indicators.[85] For the past several years, the Department joined many organizations in sharing information about cybersecurity threats, but the sharing was primarily conducted through humans – that is, a company or security researcher would identify a vulnerability and either send an email to the NCCIC or call the service desk.[86] Analysts would then review the information, compare it to other data available to the NCCIC, and, if appropriate, email it to various organizations for their action. This form of information sharing has been important; for the first time, organizations have begun sharing critical data between each other, with the government, across sectors and across governments.[87]

While significant, this form of sharing involves humans and therefore does not move at the speed necessary. Therefore, the Department began to pilot an automated capability, where machines could communicate important cybersecurity threats and measures to defend against those threats directly with other machines. The Automated Indicator Sharing (AIS) initiative was designed to be a capability that receives, processes, and disseminates cyber threat indicators in real-time.[88]

In December of 2015, Congress turned this initiative into a mandate. Under the Cybersecurity Act of 2015, the Department of Homeland Security is required to "develop and implement a capability and process" that "shall accept from any non-Federal entity in real time cyber threat indicators and defensive

---

83 *Id.*

84 The Cybersecurity Act of 2015, Pub. L. No. 114-113, 129 Stat. 2242 (2015).

85 Press Release, The White House, Presidential Policy Directive—Critical Infrastructure Security and Resilience: PPD-21, (Feb. 12, 2013) (on file with author).

86 *National Cybersecurity and Communications Integration Center*, DHS.GOV, https://www.dhs.gov/national-cybersecurity-and-communications-integration-center (last visited Oct. 14, 2016).

87 *Id.*

88 *Automated Indicator Sharing (AIS)*, DHS.GOV, https://www.dhs.gov/ais (last visited June 21, 2016).

measures."[89] The DHS capability shall "be the process by which the Federal Government receives cyber threat indicators and defensive measures . . . that are shared by a non-Federal entity with the Federal Government . . . ."[90] DHS was directed to receive those submissions by electronic mail, an interactive form on an Internet website, or through a "real time, automated process between information systems . . . ."[91]

Under the law, the Secretary of Homeland Security was required to certify to the Congress that the automated process was functional:

> [T]he Secretary of Homeland Security shall . . . submit to Congress a certification as to whether the capability and process required by paragraph (1) fully and effectively operates . . . [as] the process by which the Federal Government receives from any non-Federal entity a cyber threat indicator or defensive measure under this title . . . .[92]

Congress established an extremely aggressive timeline: this certification had to be made within 90 days of the date of enactment.[93] Because the Department had been working on AIS, the Secretary was able to meet the Congressional mandate and certify that a "real time, automated process" is operational.[94] Thus, the Department has initiated what will hopefully become a multi-directional information sharing environment, allowing governments, companies and academia to block malicious intrusions before they occur.

Types of Information to be Shared

The Cybersecurity Act defines the specific types of information that can be shared under the real time process. The Act establishes two types of information that can be shared: "cyber threat indicators" and "defensive measures."[95] Each of these is very carefully defined. The term "cyber threat indicator," or CTI, is defined in eight sub-parts, as information that is necessary to describe or identify:

> Malicious reconnaissance, including anomalous patters of communication that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
>
> A method of defeating a security control or exploitation of a security vulnerability;
>
> A security vulnerability, including anomalous activity that appears to indicate the

89 Cybersecurity Information Sharing Act, 6 U.S.C.A. § 1504(c)(1) (West 2016).
90 *Id.* at § 1504(c)(1)(B).
91 *Id.*
92 *Id.*
93 *Id.* at § 1504(c)(2)(A).
94 *Automated Indicator Sharing (AIS)*, US-CERT., https://www.us-cert.gov/ais (last visited Oct. 4, 2016).
95 6 U.S.C.A. § 1501(6) & (7).

> existence of a security vulnerability;
>
> A method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
>
> Malicious cyber command and control;
>
> The actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
>
> Any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
>
> Any combination thereof.[96]

Guidance produced by the Departments of Justice and Homeland Security provides specific examples that help explain the term "cyber threat indicator."[97] A CTI could include a software publisher that reports on a vulnerability that it has discovered in its software; a security researcher that reports on the domain names or IP addresses associated with botnets; a company experiencing a distributed denial of service attack to its public-facing website could report the IP addresses that seem to be sending the malicious traffic; or, a managed security service company could submit a pattern of domain name lookups that it believes correspond to malware infections.[98]

CSA also required that "defensive measures" should be included in the real-time sharing environment. This complex term is defined in the statute: "[A]n action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability." [99]

The DOJ/DHS guidance also tries to more specifically define the concept of defensive measures by citing several examples, including: an individual could share with others a computer program that identifies a pattern of malicious activity in web traffic; a method for loading signatures into a company's intrusion detection system; or a firewall rule that prevents certain types of traffic from entering a network.[100]

---

96 *Id.* at § 1501(6).

97 DEP'T OF HOMELAND SEC. & DEP'T OF JUSTICE, GUIDANCE TO ASSIST NON-FED. ENTITIES TO SHARE CYBER THREAT INDICATORS & DEFENSIVE MEASURES WITH FED. ENTITIES UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 4 (2016), https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf [hereinafter DHS & DOJ GUIDANCE].

98 *Id.*

99 6 U.S.C.A. § 1501(7).

100 DHS & DOJ GUIDANCE, *supra* note 97, at 7.

Incentives to Share

Congress recognized that the private sector had to overcome a number of potential obstacles if companies are to participate in this information sharing environment. Therefore, CSA explicitly states that if a company shares CTIs or defensive measures, it "shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection."[101] Moreover, proprietary information can be protected: "a [CTI] or defensive measure …shall be considered the commercial, financial, and proprietary information of such non-Federal entity[.]"[102] Such communications will also be exempt from disclosure under the Freedom of Information Act and state and local disclosure laws.[103] This type of information sharing will not be considered an *ex parte* communication with a federal administrative decision-making official.[104] The statute also makes clear that these communications will not be considered an anti-trust violation for companies to join together to share cyber threat information.[105] Finally, the incentive that received the most notice and commentary was the Act's liability protections. CSA provides that "[n]o cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure[.]"[106]

Sharing within the Federal Government

Congress wanted to ensure that DHS would pass the cyber threat information it receives on to other federal agencies with responsibilities in this arena. Therefore, the CSA requires that DHS "ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators and defensive measures shared through the real-time process[.]"[107] The Act also made clear that the automated process is not to be the exclusive method for the private sector to share cyber information with the Federal government – organizations are free to continue to share information with law enforcement, if they have statutory obligations to report such information, or if they have contractual requirements to share such information.[108]

---

101 6 U.S.C.A. § 1504(d)(1).
102 *Id.* at § 1504(d)(2).
103 *Id.* at § 1504(d)(3)(B).
104 *Id.* at § 1504(d)(4).
105 *Id.* at § 1503(e)(1).
106 *Id.* at § 1505(b).
107 Cybersecurity Information Sharing Act, 6 U.S.C.A. § 1504(c)(1)(C) (West 2016).
108 Cybersecurity Information Sharing Act, 6 U.S.C.A .§ 1504(c)(1)(E) (West 2016).

Perceived Challenges

There were, of course, a number of challenges raised as an information sharing environment on cyber threats was discussed. One of the key concerns was aggressively advocated by a number of civil liberties and consumer groups: that the government should not be empowered to accumulate vast treasure troves of data. The advocates were concerned that CTIs and defensive measures would include sensitive Personally Identifiable Information, and that the government would not adequately protect this information. As a corollary, there was concern that proprietary information of companies also would be accumulated by government and sloppily handled.

One letter written by advocates several months before the legislation passed the Congress highlights the concerns:

> Revelations about the National Security Agency's secret collection of the personal information of millions of Americans highlighted the critical need for more oversight of government intelligence agencies and protections of consumers' sensitive personal information. Common sense would tell us that expanding opportunities for government surveillance is not the solution . . . Rapid and expansive sharing of cyber threat data between corporations and government agencies without sufficient safeguards will increase the risk of misuse of that information.[109]

Many agencies are at the forefront working together, implementing, and hosting this new real time, automated capability. Because of the investment that DHS made to build its privacy, civil rights and civil liberties structures, the Administration and the Congress ultimately decided that DHS should be the host.[110] Cong. Michael McCaul, Chairman of the House Homeland Security Committee, said, "DHS has some of the strongest privacy protection mechanisms in the federal government . . . . [and] [s]uch built-in privacy oversight is an important reason why DHS is the leading civilian interface for these exchanges."[111] Therefore, DHS's privacy and civil liberties structures were put to the test by the requirements of the Cybersecurity Act of 2015.

C. Privacy and Civil Liberties Protections

Congress and the Department of Homeland Security took action to address the privacy and civil liberties concerns that had been one of the most substantial barriers to passage of CSA. Congress inserted policy and operational pa-

---

109 Letter from Center for Democracy & Technology et al., Consumer Advocates, to Hon. Mitch McConnell, Senator, U.S. Senate (Oct. 21, 2015), https://cdt.org/files/2015/10/CISA_Letter_10.21.15.pdf.

110 Cybersecurity Information Sharing Act, 6 U.S.C.A §1504(c)(1)(C) (West 2016).

111 Michael McCaul, Chairman, U.S. Committee on Homeland Security, Safeguarding the Digital Frontier: The Way Ahead for American Cybersecurity and Civilian Network (Mar. 17, 2015) (transcript on file with author).

rameters, while the Department focused on the design of AIS.

Policy and Operational Parameters

Congress established limitations on how information can be shared. The law requires federal entities to review and remove any information that is shared to ensure that unnecessary personally identifiable information is not provided to the government. This can be accomplished through human review (Section 1502(d)(2)(A)) or through a "technical capability configured to remove any personal information . . . not directly related to a cybersecurity threat[.]"[112]

Congress also inserted limitations on how cyber threat information can be used. It required that information can be disclosed to, retained by, and used by any Federal agency only for "a cybersecurity purpose."[113] The only exception is if a government agency believes that information shared will be relevant to "an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction."[114] If a company shares cyber threat information that implicated a "serious threat to a minor, including sexual exploitation and threats to physical safety," then the government can use it to prevent, investigate, disrupt or prosecute any such crime.[115]

Congress also ensured that there would be extensive audits and reviews.[116] The Inspectors General of the agencies implementing AIS must submit a report every 2 years to the Congress that includes an "assessment of the sufficiency of the policies, procedures, and guidelines . . . . relating to the removal of information not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual."[117] Moreover, within 3 years after the passage of the CSA the Comptroller General is required to submit to Congress a report "on the actions taken by the Federal Government to remove personal information from cyber threat indicators or defensive measures[.]"[118]

Congress also required the Departments of Homeland Security and Justice to join together to write guidelines to set parameters for the design of the capability. CSA requires that the Executive Branch issue 4 sets of guidance surrounding this program: guidance to the private sector for how it can participate in the

---

112 *Id.* at § 1504(b)(1)(E)(ii).
113 *Id.* at § 1504(d)(5)(A)(i).
114 *Id.* at § 1504(d)(5)(A)(iv).
115 *Id.* at § 1504(d)(5)(A)(v).
116 *Id.* at § 1506(b)(2)(B)(i)-(iv).
117 *Id.* at § 1506(b)(1).
118 *Id.* at § 1506(c).

information sharing offered by AIS;[119] guidance to federal agencies for how they can participate;[120] guidance for federal agencies for how to handle CTIs that the agencies receive;[121] and, guidance "relating to privacy and civil liberties which shall govern the receipt, retention, use and dissemination of cyber threat indicators[.]"[122]

Through these guidelines, Congress required that the new machine-to-machine capability had to be designed with a number of core privacy and civil liberties in mind, including:

> Ensuring that the seven foundational "Fair Information Privacy Principles" had to be incorporated into the design;
>
> Limiting the length of time that a CTI containing personally identifiable information may be retained;[123]
>
> Notifying entities participating in AIS if they submit information that does not qualify as a CTI under the act;[124] and,
>
> If any personally identifiable information has to be included with a CTI, ensure it is protected throughout the information sharing environment "to the greatest extent practicable."[125]

The DHS/DOJ Guidance builds on these principles by instructing companies to limit the information they attempt to share with the government.[126] The Guidance does not leave this as a general concept, but goes into detail on specific types of information that could contain personally identifiable information and therefore should not be shared, including:

> Protected Health Information, including anything in the company's files that relates to an individual's past, present, or future physical or mental health, and to that individual's possible payment for medical services;
>
> Human Resource Information, defined to include sensitive data in an employee's personnel file;
>
> Consumer Information/History, including information regarding goods an individual purchases and personal credit;
>
> Education History, referencing the Family Educational Rights and Privacy Act (FERPA);
>
> Financial Information, including "anything from bank statements, to loan information, to credit reports;"

---

119 DHS & DOJ GUIDANCE, *supra* note 97, at 4.

120 6 U.S.C.A. § 1502(a); DHS & DOJ GUIDANCE, *supra* note 97, at 4.

121 6 U.S.C.A. § 1504 (interim guidance must be published within 60 days of enactment and final guidance must be published within 180 days of enactment); DHS & DOJ GUIDANCE, *supra* note 97, at 3.

122 6 U.S.C.A § 1504(b)(2)(A) (interim guidance must be published within 60 days of enactment and final guidance must be published within 180 days of enactment); DHS & DOJ GUIDANCE, *supra* note 97, at 3.

123 6 U.S.C.A. § 1504(b)(3)(B).

124 *Id.* at § 1504(b)(3)(E).

125 *Id.* at § 1504(b)(3)(F).

126 DHS & DOJ GUIDANCE, *supra* note 97, at 3-4.

> Information about property ownership; and, finally,
>
> Information on children under the age of 13 (citing the Children's Online Privacy Protection Act (COPPA)).[127]

Building Privacy Principles into AIS

All of these procedural limitations included in the statute were sensible. However, these directions would not have been sufficient by themselves; fundamental steps need to be taken to address the privacy and civil liberties concerns. Because the Department had invested heavily in privacy expertise and in ensuring that these privacy experts were embedded in the cybersecurity program offices at the Department, it was possible and natural to insert privacy professionals into the design of the capability. The capability had to be built by privacy professionals with privacy principles in mind.

The work actually began after the passage of the NCPA in 2014, as DHS began to develop the contours of a real-time automated machine-to-machine sharing capability.[128] At that time, the NPPD Privacy Office[129] conducted an extensive Privacy Impact Assessment of AIS; the PIA was first version was published just weeks before the Cybersecurity Act of 2015 was enacted, and an updated version was published 90 days after the law was passed.[130]

With the parameters laid out in the statute, the DHS/DOJ Guidance, and the PIA, DHS's design team went to work. The team designed AIS with stages in mind: the capacity to share or disseminate CTIs; and the capacity to receive CTIs from others, then filter or sanitize data that is received, perform any human analysis that is necessary; and disseminate those CTIs.[131] Receiving CTIs from the private sector is what most worried civil liberties advocates, particularly whether companies would indiscriminately share personal information with the government.[132] The AIS design team decided to limit even the possibility that PII could be shared by leveraging a structured format that allows

---

127 DHS & DOJ GUIDANCE, *supra* note 97, at 9-10

128 *See supra* pp. 15-16; *Oversight of the Cybersecurity Act of 2015: Before the Subcomm. On Cybersecurity, Infrastructure Prot., and Sec. Techn. Of the H. Homeland Sec Comm.*, 114 Cong. 4 (June 15, 2015) (statement of Matthew J. Eggers, Exec. Dir., Cybersecurity Police, U.S. Chamber of Commerce).

129 DEP'T OF HOMELAND SEC., NPPD AT A GLANCE 1 (2013), https://www.dhs.gov/sites/default/files/publications/nppd-at-a-glance-071614.pdf.

130 DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED INDICATOR SHARING (AIS) DHS/NPPD/PIA-029(A) 1 (2016), https://www.us-cert.gov/sites/default/files/ais_files/PIA_NPPD-AIS.pdf [hereinafter PRIVACY IMPACT ASSESSMENT].

131 *Id.* at 1-2.

132 *See supra* p. 20.

inputs only in certain fields.[133] That is, the capability only allows machines to insert certain fields of data into what is referred to as the AIS Profile, and very few fields even allow the insertion of personally identifiable information. The DHS/DOJ Guidance explains, "[S]tandardized fields in structured formats can be used to establish a profile that limits the type of information in a cyber threat indicator[.] DHS's Automated Indicator Sharing (AIS) initiative uses this means of controlling the type of information that may be shared using the automated system[.]"[134]

By limiting the information that can be submitted, the design team was able to resolve many of the core concerns. For example, the DHS/DOJ guidance states that a spear phishing email might be the source of a possible CTI. In the alleged phishing email, the "from" or "sender" line of the email would be critical for analysts to have; they must be able to understand who the sender is. If there is a malicious URL in the body of the email, that is also critical to analysts. Analysts would also need to be given access to any malware files that are attached to the email, and possibly to the "subject" line.[135] However, information in the "to" is not particularly relevant to the investigation and could contain personally identifiable information. The guidance states, "The name and e-mail address of the targets of the email (i.e., the "To" address), however, would be personal information not directly related to a cybersecurity threat and therefore should not typically be included as part of the cyber threat indicator."[136] The PIA concludes that

> "Much of the information within an indicator is centered on an observable fact about the cyber threat. For example, a cyber threat indicator has a variety of observable characteristics: a malicious email, internet protocol (IP) addresses, file hashes, domain names, uniform resource locators (URLs), malware files, and malware artifacts (attributes without a file). The specificity and nature of the observable facts are designed to reduce the risk that a cyber threat indicator contains personal content or information inappropriate to share."[137]

The story is similar with defensive measures. As the term is defined in statute, it does not include information that can be personally identifiable; instead, "it will generally consist principally of technical information that can be used to detect and counter a cybersecurity threat."[138]

Therefore, extensive precautions were taken to ensure that personally identifiable information would not be submitted. If it is, the AIS capability reviews and sanitizes information received to ensure that scrubs are done before any

---

133 *AIS*, *supra* note 95.
134 DHS & DOJ GUIDANCE, *supra* note 97, at 6.
135 *Id.* at 5.
136 *Id.*
137 *Id.* at 6.
138 *Id.* at 7.

data is disseminated.[139] DHS employs various sanitization techniques to remove any remaining PII not necessary to understanding the cyber threat.[140] If an automated technique is not available and/or able to remove PII within a data element, then that data element is placed in a queue for human review and not shared until appropriately resolved. As the PIA states,

> "DHS uses the AIS Profile to standardize the indicator and defensive measure information and implement a series of automated and manual processes to ensure that unrelated information is removed from the cyber threat indicator or defensive measure before it is disseminated to the AIS participants. Using the AIS Profile in this manner further minimizes privacy, civil liberties, and other compliance risks that may arise when PII and other sensitive information is submitted."[141]

Designing the capability in this manner presented more than privacy and civil liberties benefits – it also enables the technology to function more efficiently. As the PIA explains, "By narrowly scoping the AIS Profile to those definitions [provided in the statute], the expected content of AIS submissions is predictable, thus more easily enabling the usage of automated privacy enhancing controls."[142]

The design of the AIS capability could only be provided by, and with the support of, privacy experts. Because they were part of the AIS design team, these concepts were built into the capability. Combined with the procedural protections included in the statute and the guidance documents, the public can be assured that the sharing of cyber threat indicators and defensive measures will be undertaken in a way that respects our core values.

CONCLUSION

Throughout the life of the Department of Homeland Security, the Office for Civil Rights and Civil Liberties and Privacy Office have made substantial contributions to improving security programs and operations. The Congress intended for these then-unique positions to help shape Departmental policy and build greater public confidence in the new Cabinet agency. The impact has been felt widely, from conditions in immigration detention facilities to reforms in watchlisting to agreements with foreign governments.

The Automated Indicator Sharing capability demonstrates that the civil liberties structures built into the Homeland Security Act significantly helps the Department as it designs new security programs. New technologies can be designed to enhance both privacy and security. When both technology and

---

139 PRIVACY IMPACT ASSESSMENT, *supra* note 130, at 1-2.
140 *Id.* at 18.
141 *Id*. at 5.
142 *Id.* at 6.

civil liberties addressed, public confidence that the government will handle data with discretion and effectiveness will greatly increase.