Personal Information as an Attack Vector: Why Privacy Should Be an Operational Dimension of U.S. National Security†

Christopher K. Dearing*

† An attack vector is a pathway or means by which a hostile actor may gain unauthorized access to a computer, network, system, or organization.

* Judge Advocate, United States Army. Presently assigned to the Legal Support Office (LSO), District of Columbia Army National Guard (DCARNG), Washington D.C., J.D., 2010, Seattle University School of Law. Previous assignments include Office of Complex Investigations, National Guard Bureau (NGB), 2019; Administrative Law Attorney, National Guard Bureau (NGB), 2016–2018; Strategic Policy Legal Advisor, NGB, 2015–2016; Operational Law Attorney-Cyber, NGB, 2014–2015; Operational Law Attorney, LSO-DCARNG, 2012–2014. Member of the bar of Washington. The author is exceptionally grateful for the generous assistance and mentorship of CAPT Todd C. Huntley (USN), Lt Col Anthony W. Burgos (USMC), and Prof. Laurie R. Blank (Emory University School of Law). This paper was submitted in partial completion of the Master of Laws requirements of the 67th Judge Advocate Officer Graduate Course. All remaining errors are my own. The views expressed are my own and do not reflect the official policy or position of the DCARNG, U.S. Army, the National Guard Bureau, Department of Defense, or the U.S. Government.

INTRODUCTION

Information has become the new currency of exchange in the cyber age,[1] and, as a whole, the U.S. government has failed to keep pace with the rapid changes within the information domain. The government has taken little or no action on the security of social media and networks,[2] despite the fact that nearly all major organizations in this field have seen, and continue to see, significant compromises of user information.[3] Commercial and health care networks have seen, and continue to see, breaches of customers' personal information,[4] and even in government itself, agencies struggle to meet current cybersecurity and privacy requirements.[5] The U.S. government dedicates significant resources to the protection of military and national security information. We prioritize the security of information on our critical infrastructure, such as energy, water, and transportation, and we look at all government information systems as important components of our national security infrastructure. Personal information, on the other hand, is not considered within this category of critical national security assets.

Federal privacy law has historically been seen as an administrative endeavor to keep government intrusion into the private lives of U.S. persons at bay. However, technology has changed significantly since the concept of privacy was first conceived. The ubiquity of information and information technology presents increasing dangers to privacy, and they present new opportunities for exploiting personal information as an attack vector on societal institutions, military

1. Andy Serwer, *Mark Warner: This Will 'Send a Shiver Down the Spine' of Facebook, Twitter, and Google*, YAHOO! FINANCE (Nov. 14, 2018), https://finance.yahoo.com/news/mark-warner-will-send-shiver-spine-facebook-twitter-google-161313831.html (As one U.S. senator stated, "data [is] the new oil.").

2. *See generally* Mark R. Warner, *Potential Policy Proposals for Regulation of Social Media and Technology Firms* (White Paper Draft), https://www.warner.senate.gov/public/_cache/files/d/3/d32c2f17-cc76-4e11-8aa9-897eb3c90d16/65A7C5D983F899DAAE5AA21F57BAD944.social-media-regulation-proposals.pdf.

3. *See, e.g.*, *infra*. Part V.

4. Calyptix, *Biggest Cyber Attacks 2017: How They Happened*, CALYPTIX SECURITY (Nov. 30, 2017), https://www.calyptix.com/top-threats/biggest-cyber-attacks-2017-happened/.

5. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-17-317, HIGH RISK SERIES: PROGRESS ON MANY HIGH RISK AREAS, WHILE SUBSTANTIAL EFFORTS NEEDED ON OTHERS 338–353 (2017).

organizations, and governments. This new attack vector has already been exploited in many ways, touching nearly every branch of the U.S. government and every federal and military employee.

Imagine if the personal information of key members of a deploying unit, intelligence organization, or government agency were exposed to attack: bank accounts were emptied, and disinformation was mingled with other pieces of their personal lives now published online. Such an attack would create havoc in their personal lives. Arguably, surgical targeting of key persons may only distract an organization in a marginal way. On the other hand, widening the attack surface (across systems or enterprises) or increasing the gravity of effects (from personal support systems to organizational response and readiness) could hinder if not cripple an organization's ability to accomplish its mission.

This paper will explore how threats to personal information have materialized into a new attack vector on society, and why the concept of privacy, as an administrative requirement within the U.S. government, should be re-conceptualized in operational terms. The defense of personal information in the cyber age needs to assume approaches, missions, and protocols that are operational in nature.

The U.S. government needs to consider how attacks on personal information can be clearly construed as attacks on the physical person, which would trigger dialogue relative to establishing new norms and, ideally, legal conventions on attacks on a citizen's digital persona. The paper recommends the (re)organization of congressional committees that better address the information environment as well as the creation of a privacy czar.

In terms of approaches, organizations need to consider personal information of employees, service members, industry partners, and their dependents as having operational value that needs to be evaluated and integrated within organizational risk assessments and planning. Privacy program officers need to assume greater responsibilities for identifying not only risks to the personal information held within organizational databases and systems, but also the extent to which employees' personal information is exposed in systems and networks outside of their immediate control. As a matter of routine, government and military personnel share sensitive personal information about themselves and their family members to a universe of information systems – most of which are *not* monitored, let alone accountable, to the U.S. government. Many, if not most, of these information systems have been and continue to be compromised by various hostile actors. In the event any of this information or these systems were part of a coordinated attack to exploit, distract, or cripple an organization, it is unclear whether organizations would even understand that their personnel, and consequently the organization, were under attack.

The U.S. government needs to begin developing doctrine and training government personnel and support staff on the threat environment and how to protect their personal information. This training should include what to do when one's personal information has been compromised, exploited, or weaponized. Currently, there is little relief in the event there is an attack on one's identity. Finally, the U.S. government should consider insurance

options that private industry could offer to personnel in the event their personal information has been exploited.

Part I of this paper will provide a historical overview of privacy law and how transformations in media and technology have shaped and compelled changes in the treatment of personal information. Part II, titled "Technological Somnambulism," will orient the reader to the vast transformation to the information landscape that has occurred in the last twenty years. Changes in information technology and how we interact with and depend on such technology have created an entirely new domain for personal life. In many ways, we are moving into a world where the digital self will be a mirror image of the physical self.

Part III will discuss the failure of the U.S. government to keep pace with these revolutionary changes. While the U.S. government has endeavored to stay abreast of emerging technologies, the scale, pace, and nature of changes in the information world have far outpaced current laws, regulations, and policies.

Part IV will describe how personal information has become a new attack vector, in which U.S. national security strategy is still contemplating a response. U.S. adversaries see asymmetric, information warfare as a key tenet to any conflict with the United States, and the Russian interference in the U.S. presidential election of 2016 is only the beginning of a new emerging doctrine tied to the weaponization of information.

Part V will provide real examples of how hostile actors are already maneuvering and taking stock of this new doctrine – capturing large troves of information that covers all elements of one's personal identity. Part VI looks at future attack vectors through a series of vignettes. Starting from well-recognized uses for espionage and ending with the use of personal information in all forms of kinetic attacks, the vignettes aim to describe how personal information could be easily wielded as a pre-emptive weapon or force multiplier in a digital Pearl Harbor.

The paper closes with a list of basic recommendations for moving forward. Although there is no comprehensive solution set to this new form of warfare, the U.S. government can reduce risk through a proactive, reflective personal information security system that re-conceptualizes personal information in operational terms.

I. HISTORICAL OVERVIEW OF PRIVACY LAW

The history of privacy law as it relates to information about people can be organized into several distinct chapters or periods that are closely associated with transformations in media and information technology. From news pamphlets to the printing press, and eventually computers, the internet, and big data, privacy law has always developed slowly and often well behind technological change.[6]

6. PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 4–5 (1995) ("In the United States, the formulation of policy to protect privacy in the face of technological change has been slow and incremental."); *id*. at xi–xii ("[I]t took years, if not decades, for Congress to formulate and adopt a policy to address the perceived problems.").

Before the introduction of the telegraph in the 1830s, the rate at which information could be collected and disseminated was largely determined by the speed of a messenger. Media was also largely bounded by what could be reproduced by the pen and paper and to a lesser extent the printing press. In this low technology environment, it is not hard to see why there were not many legal remedies for loss, compromise, or damage to one's personal information or privacy. If records about one's person and identity were largely confined to birth, marriage, and property paper records, then there really were not many concerns of harm on account of improper disclosures or handling of personal information. The primary relief one could hope to obtain in the event of reputational or identity harm would be in a common law action of slander.[7]

With the arrival of the telegraph and proliferation of print news media in the mid-1800s, discussions on privacy centered on concerns about the protection of a person's reputation and emotional self in the face of sensational journalism. The mid-1800s saw an explosion in the number of newspapers and newspaper readers. From 1850 to 1890, newspaper production grew 1,000 percent and readership increased from 800,000 readers in 1850 to 8 million readers in 1890.[8] In the 1880s, there was also an upwelling of popular disapproval toward the excesses of yellow journalism, which targeted the private lives of famous people and their families. Nowhere was this new consideration of privacy better elaborated than in a law review article written by Samuel D. Warren and Louis D. Brandeis in December 1890.[9]

Warren and Brandeis described the right to privacy as a common law right that required protection in the face of technology and enterprises that increasingly encroached upon the personal lives of people. "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[10] Warren and Brandeis' concept of privacy centered on the protection of an individual's intangible, emotional self, which was not covered by the laws of slander or libel.[11] Though these common law actions extended the sphere of protection for an individual's emotional, mental, or sensory well-being, they offered a legal remedy for only those injuries that were by nature "material rather than

7. *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 194, n.3 (1890) (describing the earliest known case of an action in slander from 1356); *see also* 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 169 (1769) (An American citizen was also protected against eavesdropping, which was defined as "listen[ing] under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales.").

8. Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY, 1–10 (PLI ed., 2006).

9. Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 1 (1979).

10. Warren & Brandeis, *supra* note 7, at 195.

11. *Id*. at 196.

spiritual."[12] In effect, contemporary law did not recognize a principle "upon which compensation can be granted for mere injury to the feelings."[13]

A third distinct chapter in the law's treatment of personal information can be found with the advent of computers and data processing systems.[14] Writing in the dissent for a 1928 wiretapping case, Supreme Court Justice Louis Brandeis stated,

> Subtler and more far reaching means of invading privacy have become available to the Government... The progress of science in furnishing the Government with the means of espionage is not likely to stop with wiretapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.[15]

The modern computer did not exist in 1928,[16] yet Justice Brandeis' opinion could not have been more prescient as to the dangers that would emerge several decades later. In the post-World War II era, computers, automated databases, and new forms of communication technology emerged and presented opportunities for increased access into, and control over, the personal lives of individuals. The physical and practical limits imposed by paper records slowly gave way to data processing, which emerged not only in government but also in big industry and commerce. "Compared with [the] pre-[World War II] years, the number of bank checks written, the number of college students, and the number of pieces of mail all nearly doubled; the number of income-tax returns quadrupled; and the number of Social Security payments increased by a factor of more than 35."[17] In the post-World War II era, American institutions were awash in records on some of the most intimate financial, property, and personal details of private citizens. This upsurge in records was part and parcel to the rise of the administrative state.

One can trace the origins of the administrative state to the late nineteenth century when the United States underwent a rapid social transformation from a

12. *Id*. at 197.

13. *Id*.; *see also* Glancy, *supra* note 9 at 2.

14. *See generally* KATHRYN E. BOUSKILL, SEIFUL CHONDE, WILLIAM WELSER, SPEED AND SECURITY: PROMISES, PERILS, AND PARADOXES OF ACCELERATING EVERYTHING, RAND 4 (2018) (discussing how different technologies – from the telephone to the internet and smartphone – were adopted in history: 1860–2020).

15. Olmstead v. United States, 277 U.S. 438, 473–74 (1928).

16. *See generally* Jo Marchant, *Decoding the Antikythera Mechanism, the First Computer*, SMITHSONIAN MAGAZINE (Feb. 2015), https://www.smithsonianmag.com/history/decoding-antikythera-mechanism-first-computer-180953979/ (describing an ancient Greek "computer" that was essentially a gear-laden device, which was believed to be capable of tracking the motions of the sun, moon, and planets).

17. SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T. OF HEALTH, EDUC. & WELFARE, DHEW PUB. NO. (OS) 73-94, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 7–8 (1973).

largely agrarian society to a vast industrial nation.[18] The excesses of the Gilded Age and unbridled capitalism compelled the federal and state governments to exercise a greater hand in economic regulation. This governmental shift from laissez-faire economics to managed capitalism reached an inflection point during the Great Depression, in which new agencies were created to rescue whole segments of society and the economy from collapse.[19] From banks and big industry to labor, food, welfare, and the environment, the federal government assumed greater responsibility for oversight and regulation over an increasingly wider spectrum of economic and social matters. With greater oversight and regulation came greater demands for personal information from the individual citizens each agency touched.

The rise of data processing and information technology contributed to, and was incentivized by, the rise of the administrative state, particularly in the 1960s and after.[20] Government agencies leveraged new information technologies to increase efficiency, power, and control over their ever-expanding administrative spheres of responsibility.

Nowhere was this trend more concerning than in the realm of law enforcement, in which police and domestic intelligence activities increasingly leveraged automated forms of storage and communication systems to collect, monitor, and maintain records on private citizens.[21] Improvements in data collection, storage, and retrieval coincided with a period of significant civil disturbances and fears of internal threats, which encouraged increased targeting of American persons by military and civilian law enforcement and intelligence agencies.

In the midst of the Cold War and fears of Communist infiltration, the Federal Bureau of Investigation (FBI) expanded its investigatory activities to cover the monitoring and surveillance of lawful activities by American persons.[22] Likewise, the Central Intelligence Agency (CIA)[23] and a host of other

18. *See generally* Eliza Wing-Yee Lee, *Political Science, Public Administration, and the Rise of the American Administrative State*, 55 PUB. ADMIN. REV. 538, 539 (1995).

19. *Id*. at 541.

20. Claire Barrett, *Guiding Principles for Information Privacy*, in U.S. GOVERNMENT PRIVACY: ESSENTIAL POLICIES AND PRACTICES FOR PRIVACY PROFESSIONALS 8 (Deborah Kendall ed., 2d ed. 2013) ("In the 1960s, the increasing power and capacity of computer systems led to proposals for, and prompted fears of, federal data banks that would centralize unprecedented volumes of PII [personally identifiable information]."); *see* LANCE J. HOFFMAN., COMPUTERS AND PRIVACY IN THE NEXT DECADE xv (1980) ("The controversy over the proposed national data bank in 1967 was one of the first events in the early warning phase of the first wave [on action on privacy]."); *see also* REGAN, *supra* note 6, at 13 ("By the mid-1960s, concerns about privacy and technology were reflected in a 'literature of alarm' that was instrumental in placing the issues of information privacy, communication privacy, and psychological privacy on the policy agenda.").

21. *See* Alan F. Westin, *The Long-Term Implications of Computers for Privacy and the Protection of Public Order*, in COMPUTERS AND PRIVACY IN THE NEXT DECADE, *supra* note 20, at 167–181 (discussing some of the implications of law enforcement use of computers).

22. *See* William H. Ware, *Privacy and Information Technology The Years Ahead*, in COMPUTERS AND PRIVACY IN THE NEXT DECADE, *supra* note 20, at 9-20.

23. *See generally* NELSON A. ROCKEFELLER ET AL., COMMISSION ON CIA ACTIVITIES WITHIN THE UNITED STATES, REPORT TO THE PRESIDENT (1975).

military intelligence agencies took on an increased role in the monitoring of individual Americans.[24]

The deluge of stories on actual and alleged government surveillance activities, combined with the public perception of secret dossiers on large numbers of U.S. persons, contributed to an atmosphere that compelled vigorous debate in Congress and throughout the federal government and academia on the concept of privacy.[25]

Amidst this debate, the Health, Education, Welfare (HEW) Advisory Committee on Automated Systems was established in 1972 to study the impact of automated data systems and their potential consequences for privacy, due process, and basic liberties.[26] The Committee found that "[u]nder current law, a person's privacy is poorly protected against arbitrary or abusive record-keeping practices."[27] For this reason, and in the interest of standardizing record-keeping procedures, the Committee recommended the adoption of a Federal "Code of Fair Information Practices."[28] The Code of Fair Information Practices for automated personal data systems was centered on five basic principles:

- There must be no personal data record-keeping systems the very existence of which is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[29]

24. *See* PAUL J. SCHEIPS, THE ROLE OF FEDERAL MILITARY FORCES IN DOMESTIC OPERATIONS, 1945–1992 398-99 (2005) (discussing the Army Intelligence Command's use of expanded intelligence collection plans on civilian groups, demonstrations, and other political activities in the United States).

25. For example, the Commission on CIA Activities Within the United States listed the initial and subsequent charges that they were tasked to investigate as it relates to the CIA's domestic activities. ROCKEFELLER ET AL., *supra* note 23, at 9 ("The initial public charges... [of] the CIA's domestic activities ... [include]: 1. Large-scale spying on American citizens in the United States by the CIA ... 2. Keeping dossiers on large numbers of American citizens. 3. Aiming these activities at Americans who have expressed their disagreement with various government policies ...").

26. SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., *supra* note 17, at viii-ix.

27. *Id*. at xx.

28. *Id*. at xxiii.

29. *Id*. at xx-xi.

The Privacy Act of 1974 incorporated these recommendations – focusing in particular on the heightened contemporary concerns of unwarranted government intrusion and control over personal information.[30] The Act required federal agencies, with limited exceptions, to provide notice to the public on the types of personal information collected, processed, stored, and used by the agency in a system of records.[31] A landmark law at the time, the Act was both a statute for giving an individual access to records about him or herself as contained within these systems of records, as well as a law to restrict agencies' collection, use, and maintenance of these records. One of the core elements of the Act is the prohibition against agency disclosure of personal information without the prior written consent of the individual to whom the information pertains.[32] The Act allowed for a limited number of exceptions to this rule,[33] and it also permitted agencies, under certain conditions, to exempt particular types of systems of records from certain requirements of the Act.[34] The Act allowed for suit against the United States when an agency fails to comply with the Act,[35] and willful violation of the Privacy Act carries criminal and civil penalties.[36] Overall, the Act established a benchmark for how agencies must handle the personal information of U.S. citizens and legal permanent residents.[37]

Since entering the age of the internet,[38] Congress passed various new laws to keep agencies' privacy programs abreast of advances in information technology. In 1988, Congress passed the Computer Matching and Privacy Protection Act,[39] which required relevant agencies to publicly disclose the written agreements they use in matching data between electronic federal Privacy Act record systems. In essence, if a federal agency wants to use the data that is held by another federal (or non-federal) agency for its use in granting or recouping financial benefits, it must have an approved, written agreement in place that has been reviewed by a

30. The Privacy Act of 1974, 5 U.S.C. § 552a (1974).

31. Many aspects of the act reflect principles and recommendations from a 1973 committee report from the U.S. Department of Health, Education, and Welfare (HEW). *See* SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., *supra* note 17, at xxv.

32. 5 U.S.C. § 552a(b).

33. *Id.* § 552a(b)(1)–(12) (For example, agencies may disclose Privacy Act records without an individual's consent as a "routine use" that is properly approved and reflected in a system of record notice or SORN, as published in the Federal Register.).

34. *Id.* § 552a(j)–(k) (discussing general and specific exemptions).

35. *Id.* § 552a(g).

36. *Id.* §§ 552a(g), (i) (discussing civil and criminal penalties).

37. *Id.* § 552a(a)(2) (defining an individual as "a citizen of the United States or an alien lawfully admitted for permanent residence").

38. U.S. government computer networks preceded commercial internet service providers, which did not come onto the scene until the 1980s. The first webpage was published on August 6, 1991. Alyson Shontell, *FLASHBACK: This Is What the First-Ever Website Looked Like*, BUSINESS INSIDER (June 29, 2011), https://www.businessinsider.com/flashback-this-is-what-the-first-website-ever-looked-like-2011-6; *see also* WORLD WIDE WEB, http://info.cern.ch/ hypertext/WWW/TheProject.html (Feb. 20, 2019) (reflecting the first web page ever created).

39. Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100–503, 102 Stat. 2507 (codified as amended at 5 U.S.C. § 552a (1988)).

data integrity board, and it also must be made available to Congress and the public.[40] In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA), which protects individually identifiable health information that is transmitted or maintained by a covered entity.[41] HIPAA requires entities in both the public and private sectors to send a breach notification to patients (and the Department of Health and Human Services) any time the protected health information of more than 500 patients has been affected. Congress has also passed a variety of other laws addressing a wide spectrum of public and private institutions involved in matters related to families, children, and financial services, to name a few.[42]

The E-Government Act[43] and the Federal Information Security Management Act (FISMA)[44] of 2002 were other significant acts intended to help bring the Privacy Act in-line with the advance of digital technology. The intent of the E-Government Act was to promote the public use of electronic government services, as well as to establish a broad framework of measures that agencies must implement to ensure the security of their information technology (IT) systems. The Act required Privacy Impact Assessments (PIAs) to be completed for any new collection of personal information as well as any time the agency seeks to develop or acquire IT to collect, maintain, or disseminate personal information.[45] The intent of the FISMA was to provide a comprehensive framework for ensuring information security over federal information systems, which included empowering chief information officers (CIOs) and chief information security officers (CISOs) in IT policy development and implementation for their respective agencies. In addition, the Act provided the National Institute of Standards and Technology (NIST) with the responsibility for establishing information security technical standards and compliance testing and reporting.[46]

In terms of regulation, different U.S. presidents have issued various executive orders in the spirit of protecting privacy and civil liberties. Executive Order 12333, which covers all intelligence activities of the federal government, is relevant to privacy insofar as it sets the framework of guidelines, restrictions, and authorities for the Intelligence Community's activities in relation to U.S. persons.[47] Executive Order 13556 is also relevant to privacy as it seeks to establish a

40. *Id.* § 2.

41. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (codified as amended in scattered sections of 42 U.S.C.).

42. *See, e.g.*, Financial Services Modernization Act of 1999, Pub. L. No. 106–102, 113 Stat. 1338 (codified as amended in scattered sections of 12 and 15 U.S.C.); Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (1974).

43. E-Government Act of 2002, Pub. L. No. 107–347, 116 Stat. 2899 (codified as amended in scattered sections of 44 U.S.C.).

44. *Id.* §§ 301-5, 116 Stat. at 2946–61.

45. *See generally* Rebecca J. Richards, *The E-Government Act*, in U.S. GOVERNMENT PRIVACY: ESSENTIAL POLICIES AND PRACTICES FOR PRIVACY PROFESSIONALS, *supra* note 20, at 29.

46. *See generally id.*

47. Exec. Order No. 12,333, 46 Fed. Reg. 59941 (Dec. 4, 1981).

system by which unclassified information, such as personally identifiable information (PII), should be handled to ensure its security.[48]

In accordance with the Privacy Act, the Office of Management and Budget (OMB) is responsible for developing and prescribing Privacy Act guidelines and regulations, as well as supervising agency compliance.[49]

To stay abreast of advances in information technology, media, and practices, OMB has published a number of circulars and memoranda ranging from privacy program development and implementation, to breach response plans and agency use of websites, social media, and software applications.[50] OMB is also responsible for reviewing and approving many agency privacy policies, and all agencies of the federal government must report to OMB on a number of privacy program implementation areas.[51]

Though not expressly stated in the Privacy Act, the Department of Justice (DOJ) also has a role in the federal government's privacy mission by providing legal guidance on court decisions. DOJ's Office of Privacy and Civil Liberties (OPCL) provides an "Overview of the Privacy Act of 1974," which discusses judicial interpretations of various provisions of the Privacy Act. As stated in the overview's preface, "[t]he Overview is not intended to provide policy guidance, as that role statutorily rests with the Office of Management and Budget (OMB). . .. However, where OMB has issued policy guidance on particular provisions of the Act, citation to such guidance is provided in the Overview."[52]

NIST implements a number of privacy and cybersecurity responsibilities, including setting technical standards for IT systems and providing guidelines on privacy and cybersecurity. Unlike OMB, NIST is considered a non-regulatory agency whose responsibilities do not include supervisory oversight. To this end, in 2013, the President issued Executive Order 13636, which directed NIST to develop a voluntary framework for reducing cybersecurity risks to critical infrastructure.[53] After significant stakeholder input, NIST published version 1.1 of this voluntary framework in April 2018.[54] NIST has also issued, among other guidance, specific protocols and standards for the incorporation of privacy controls

48. Exec. Order No. 13,556, 75 Fed. Reg. 68675 (Nov. 4, 2010).

49. The Privacy Act of 1974, 5 U.S.C. § 552a(v) (1974).

50. *See* OFFICE OF MGMT. & BUDGET, PRIVACY, https://www.whitehouse.gov/omb/information-regulatory-affairs/privacy/ (listing and describing OMB guidance).

51. For example, OMB Memorandum M-03-22 requires agencies to report annually on FISMA Section 208 compliance. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB M-03-22, OMB GUIDANCE FOR IMPLEMENTING THE PRIVACY PROVISIONS OF THE E-GOVERNMENT ACT OF 2002 (2003).

52. OFFICE OF PRIVACY & CIVIL LIBERTIES, DEP'T OF JUSTICE, OVERVIEW OF THE PRIVACY ACT OF 1974 (2015), https://www.justice.gov/opcl/file/793026/download.

53. Exec. Order No. 13,636, 78 Fed. Reg. 11737 (Feb. 12, 2013).

54. NAT'L INST. STANDARDS & TECH., U.S. DEP'T. OF COMMERCE, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2018).

within IT systems within the federal government.[55] As of November 2018, NIST is in the midst of updating Appendix J, its Privacy Control Catalog of NIST Special Publication 800–53, and it is developing the NIST Privacy Framework as a separate, but complementary, voluntary tool to assist agencies in identifying and managing enterprise-wide privacy risks.[56]

Within the Department of Defense (DoD), the Deputy Chief Management Officer (DCMO) serves as the DoD Privacy and Civil Liberties Officer (PCLO). Under sections 2000ee-1 and 2000ee-2 of Title 42 of the U.S. code, the PCLO serves as the principal advisor to the head of the department on privacy and civil liberties.[57] DoD also has a Senior Agency Official for Privacy (SAOP), who is responsible for "taking a central role in overseeing, coordinating, and facilitating DoD's privacy and civil liberties compliance efforts, consistent with applicable law, regulation, and policy."[58] The Chief, Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD) assists the DPCLO and the SAOP in their responsibilities, as well as overseeing and implementing the DoD Privacy and Civil Liberties Programs.[59] Within DoD components, there must be a Component Senior Official for Privacy (CSOP) to support the SAOP, as well as a component privacy officer to administer the DoD privacy program for the component on behalf of the CSOP.[60]

The individual military services also publish their own privacy program guidance in the form of regulations and public rules in accordance with DoD's guidance. While each service has generally crafted their privacy programs to fit within their respective organizational structure, they have tended to borrow heavily from the language of DoD's guidance.

Under current regulations, privacy program managers and information security officers are responsible for shepherding compliance, risk assessments, and response, and lawyers' official roles are reserved for the general function of answering questions of law and regulation as they arise.

Moving from the federal government to the private sector, there are a number of different entities involved to some degree in the regulation of Federal privacy law. One of the most prominent agencies involved in the enforcement of federal privacy law is the Federal Trade Commission (FTC). The FTC is the chief federal agency for the regulation and enforcement of privacy law as it relates to financial transactions and consumer affairs.[61] In terms of function, the agency uses law

55. *See* NAT. INST. STANDARDS & TECH., DEP'T OF COMMERCE, NIST SPECIAL PUB. 800-53, SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS 4 (2013).

56. Webinar, *Q&A on the NIST Privacy Framework*, NAT'L INST. OF STANDARDS & TECH. (Nov. 29, 2018), https://www.nist.gov/news-events/events/2018/11/nist-privacy-framework-qa-webinar.

57. U.S. DEP'T OF DEF., INSTR. 5400.11, DOD PRIVACY PROGRAM 5 (2019).

58. *Id*. at 5–6.

59. *Id*. at 7–8.

60. *Id*. at 10.

61. FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY AND SECURITY, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security.

enforcement, policy initiatives, and consumer and business education to protect consumers' personal information. In addition, the FTC is responsible for regulating entities that interact with families and children online through the Children's Online Privacy Protection Act.

II. "TECHNOLOGICAL SOMNAMBULISM"[62]

The age of big data, artificial intelligence, and the internet-of-things constitutes a new chapter in the history of information technology. Greater segments of life and reality are translated or transformed into analyzable information bits and transactions. From shopping, banking, and commerce, to all aspects of social interactions, personal activities, and routines, big data has impacted every corner of the world. "Digital ecosystems," where "users can enjoy an end-to-end experience for a wide range of products and services[,]" are increasingly dominating commercial and contractual relationships.[63] Stephen Levy, a senior writer for Wired Magazine, stated, "Every bit of data, no matter how seemingly trivial, has potential value."[64] Shoshana Zuboff, who is an author on many notable works related to technology's impact on society stated that seemingly trivial information on one's personal interests, preferences, or habits has become a new commodity that can be collected, aggregated, abstracted, analyzed, and sold.[65]

Apart from big data, advances in artificial intelligence and the internet-of-things have also begun to touch larger portions of life and reality. Data from sensors within a widening array of devices, bodies, and structures have become the source of an ever-evolving "computer-mediated" life.[66] Artificial intelligence (AI), which refers to the "ability of machines to exhibit humanlike intelligence,"[67] is also rapidly evolving. In the last several years, AI has evolved from performing basic functions like "text, speech, or image recognition," to autonomous vehicles, virtual agents, and machine learning.[68]

In many ways, the digital landscape is moving faster than one can comprehend, let alone measure and respond to.[69] In economic terms, these changes can be seen

62. *See* LANGDON WINNER, THE WHALE AND THE REACTOR: A SEARCH FOR LIMITS IN AN AGE OF HIGH TECHNOLOGY 5–10 (1986) (describing the absence of societal inquiry and understanding of the nature and significance of technology's impact on the human condition).

63. Venkat Atluri et al., *Competing in a World of Sectors Without Borders*, *in* ANALYTICS COMES OF AGE 8 (McKinsey Analytics ed., 2018).

64. Steven Levy, *Secret of Googlenomics: Data-Fueled Recipe Brews Profitability*, WIRED (May 22, 2009), https://www.wired.com/2009/05/nep-googlenomics/.

65. Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 79 (2015).

66. *Id*. at 78.

67. Tera Allas et al., *Artificial Intelligence is Getting Ready for Business, but are Businesses Ready for AI?*, *in* ANALYTICS COMES OF AGE, *supra* note 63, at 19.

68. *See id*.

69. *See* Nick Ismail, *The Top Five Big Data Trends Coming in 2018*, INFORMATION AGE (Dec. 13, 2017), https://www.information-age.com/top-five-data-trends-2018-123470020/; Nathan McDonald, *Social in 2028: Thought Leadership*, WE ARE SOCIAL BLOG (July 26, 2018), https://wearesocial.com/blog/ 2018/07/social-in-2028 (citing entry by Jim Coleman, CEO of We Are Social in London: "Let's face it, based on the rate of digital evolution in the past 10 years, no one knows what the 'new' will be in

in terms of an expansion of the internet economy and electronic commerce (e-commerce) as well as rapid shifts from desktop to mobile internet sales. In 2016, the internet economy was estimated to be over $4.2 trillion in the G-20 economies,[70] and e-commerce sales reached over $389 billion in the United States alone.[71] By 2019, mobile internet retail sales are projected to reach 50 percent of total e-commerce worldwide, and by 2022, overall e-commerce is expected to reach over 70 percent of the world retail market.[72] According to the investment bank UBS, the artificial intelligence industry generated $5 billion in revenue in 2015.[73] By 2020, UBS predicts artificial intelligence will become a $12.5 billion industry.[74]

The increase in e-commerce coincides with a transformational shift from tangible to intangible market economies. In *Capitalism Without Capital*, Jonathan Haskel and Stian Westlake describe a steady shift that has been occurring over the past twenty years in the developed world, in which investments in intangible assets are overtaking tangible investments in more countries.[75] "The market value of Apple, Amazon, Alphabet, Microsoft, and Facebook is about US$4.2 trillion, with total tangible assets amounting to about five percent (US$225 billion) of that figure." Such a ratio between tangible and intangible assets would be unheard of twenty years ago. In measuring intangible assets, "goodwill" and "brand recognition" can carry as much or more value than physical materiel, facilities, and real property.[76]

The scale, pace, and nature of change are accelerating too.[77] According to one digital research firm, over 4 billion people in the world used the internet in 2018, which reflects a 7 percent increase from the prior year.[78] Based on another

---

10 years[']time but what is almost certain is that the platforms dominating today will become deeper embedded into the fabric and everyday function of our lives."); *see also* BOUSKILL, CHONDE & WELSER, *supra* note 14, at 5 ("In the past, the slower pace of technological development and adoption allowed time for social norms, policies, education, and ethics to adapt. The current phase of acceleration is placing strain on these domains and potentially creating novel security threats with profound consequences.").

70. DAVID DEAN ET AL., BOSTON CONSULTING GROUP, THE INTERNET ECONOMY IN THE G-20: THE $4.2 TRILLION GROWTH OPPORTUNITY 3 (2012).

71. UNITED STATES CENSUS BUREAU, U.S. DEP'T OF COMMERCE, E-STATS 2016: MEASURING THE ELECTRONIC ECONOMY (2018).

72. Euromonitor Communications, *E-Commerce Is the Fastest Growing Global Retail Channel Through 2022*, EUROMONITOR INTERNATIONAL (Dec. 12, 2017), https://blog.euromonitor.com/e-commerce-is-the-fastest-growing-global-retail-channel-through-2022/.

73. UBS, AI'S COMING OF AGE, https://www.ubs.com/microsites/artificial-intelligence/en/ai-coming-age.html (Feb. 4, 2019).

74. *Id.*

75. *See generally* JONATHAN HASKEL & STIAN WESTLAKE, CAPITALISM WITHOUT CAPITAL 15 (2018) (The authors describe intangible assets as "investment in ideas, in knowledge, in aesthetic content, in software, in brands, in networks and relationships.").

76. Rohinton P. Medhora, *Rethinking Policy in a Digital World, Policy Brief No. 143*, CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION, Nov. 2018, at 2.

77. McDonald, *supra* note 69 (citing entry by Ottavio Nava, Stefano Maggi & Gabriele Cucinella: "In the next 10 years, it's very likely the speed of change will increase even more. . .").

78. Simon Kemp, *Digital in 2018: World's Internet Users Pass the 4 Billion Mark*, WE ARE SOCIAL (Jan. 30, 2018), https://wearesocial.com/blog/2018/01/global-digital-report-2018.

estimate from 2017, over 70 percent of internet users in the world also access social media sites on a regular basis.[79] In December 2018, the United Nations Agency for Information and Communication Technologies proudly announced that for the first time in history more than half of the global population is online.[80] In the same year, the number of monthly active users of Facebook, a social media platform, reached 2.2 billion people and approximately 1.45 billion people use the network on a daily basis.[81] Google, which sits at the top of big data analytics services,[82] hit approximately 3.5 billion searches per day in early 2019.[83] The market for the internet-of-things is also predicted to produce by 2025 over $11.1 trillion in economic growth and efficiency gains.[84]

Transformations in technology unsurprisingly correspond to transformations in social and business practices, protocols, and behaviors. As the amount of data on individual persons and entities increase, there will be ever-increasing opportunities and incentives to leverage such data for more efficient and effective advertising and delivery of products and services.[85] Experts in the field of social media predict the next ten years will see more "precision targeting" of individuals to create a more "personalised product experience."[86] As one social media expert states, "Social Media will die. . .[and] [t]here will be the shift to more personalised [sic] spaces, and hyper-personalisation[,]" in which interactions with consumers will be tailored to the most granular details of each person's particular activities, needs, or interests.[87] "All outgoing and incoming content will be tailored based on a cocktail of profile data," which will most likely be informed by artificial intelligence.[88]

79. *eMarketer Updates Worldwide Social Network User Figure*, EMARKETER (Jan. 16, 2018), https://perma.cc/U296-EQFU.

80. AFP, *More than Half of Global Population Now Online: UN*, YAHOO! NEWS (Dec. 7, 2018), https://sg.news.yahoo.com/more-half-global-population-now-115946999.html.

81. Al Jazeera News, *Number of Active Facebook Users Increased Despite Scandals*, AL JAZEERA (Apr. 26, 2018), https://www.aljazeera.com/news/2018/04/number-active-facebook-users-increased-scandals-180426073628185.html.

82. *See* Danny Sullivan, *Google Still World's Most Popular Search Engine By Far, But Share of Unique Searchers Dips Slightly*, SEARCH ENGINE LAND (Feb. 11, 2013), https://searchengineland.com/google-worlds-most-popular-search-engine-148089 (according to a study done in December 2012, Google held 65.2% share of the search market).

83. *See* INTERNET LIVE STATS, GOOGLE SEARCH STATISTICS, http://www.internetlivestats.com/google-search-statistics/.

84. GLOBAL COMMISSION ON INTERNET GOVERNANCE, ONE INTERNET i (2016), https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf.

85. *See, e.g.*, JEFFREY ROTHFEDER, PRIVACY FOR SALE: HOW COMPUTERIZATION HAS MADE EVERYONE'S PRIVATE LIFE AN OPEN SECRET 17 (1992) (describing how in 1992 there are "upwards of five billion records . . . in the United States that describe each resident's whereabouts and other personal minutiae.").

86. McDonald, *supra* note 69, (citing entry by Nathan McDonald, Co-Founder and Global CEO of We Are Social: *The Age of Data-Driven Connectivity*).

87. *Id.* (citing entry by Roberto Garcia, Managing Director of We Are Social in Munich & Berlin).

88. *Id.*

Profile data will not only include a person's deliberate offering of information on his or her background, actions, or interests, but inadvertent data that is collected from the ever-increasing internet-of-things. "Every day, consumers are interacting with technological devices, online platforms, and applications," which collect information on location, health, financial status, and behaviors – often without the person's express consent.[89]

In the face of such rapid technological transformation, numerous outspoken leaders in academia, commerce, culture, and politics have raised alarm over the unpreparedness of human society. In describing the rise of artificial intelligence, former U.S. Secretary of State Henry Kissinger stated, "Philosophically, intellectually – in every way – human society is unprepared for the rise of artificial intelligence."[90] "Over the next 50 years, we will see new kinds of threats to privacy that don't find their roots in totalitarianism, but in capitalism, the free market, advanced technology, and the unbridled exchange of electronic information."[91] Concurring with this assessment, former Secretary of State Hillary Clinton stated that we are unprepared for when "everything we know and everything we say and everything we write is. . .recorded somewhere."[92] As Kissinger predicts, "The Enlightenment started with essentially philosophical insights spread by a new technology. Our period is moving in the opposite direction. It has generated a potentially dominating technology in search of a guiding philosophy."[93]

III. THE ECHO CHAMBER OF U.S. GOVERNMENT AND INDUSTRY INFORMATION PRACTICES

While the U.S. government has taken steps to stay abreast of advances in information technology, media, and practices, the scale, pace, and nature of such revolutionary changes in the information world have far outpaced current laws, regulations, and policies, regardless of sector.

In the federal government sector, the Privacy Act operates as the foundational law for the federal government on privacy.[94] Subsequent legislation and rules addressing privacy are essentially tailored to update the Privacy Act's core principles. These core principles, which drew from the Code of Fair Information Practices,[95] place significant trust in the theory that individuals can be empowered to regulate how federal agencies collect, use, and share their information so long

89. Kristen L. Walker, *Surrendering Information Through the Looking Glass: Transparency, Trust, and Protection*, 35 J. PUB. POL'Y & MARKETING 144, 144 (2016).

90. Henry A. Kissinger, *How the Enlightenment Ends*, THE ATLANTIC (June 2018), https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/.

91. SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 3 (2000).

92. James Vincent, *Hillary Clinton Says America Is 'Totally Unprepared' for the Impact of AI*, THE VERGE (Nov. 23, 2017), https://www.theverge.com/2017/11/23/16693894/hillary-clinton-ai-america-totally-unprepared.

93. Kissinger, *supra* note 90.

94. Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 23 (2000).

95. SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., *supra* note 17, at xx-xxi.

as there is notice, and in some instances express consent, on these practices. State laws on privacy tend to look to the Federal Privacy Act as a model – though, in reality, the majority of states lack omnibus privacy acts.[96] While there are many similarities between the states' database security laws, material differences can include, among other things:

> [D]efinition of personal information covered by the statute; the definition of a breach; exceptions for providing notice because of the lack of materiality or risk of harm associated with the breach; whether and to the extent encrypted data is exempted from a breach; timing requirements for providing notice to individuals; the contents of a notice; the circumstances under which notice is to be provided to regulators, the media, credit reporting agencies or law enforcement; and whether or not there is an individual right of action associated with a breach of the statute.[97]

In the private sector, where legislation and rulemaking are significantly scarcer, the United States predominantly relies on industry self-regulation. "Americans tend to be more trusting of the private sector and the free market to protect personal privacy – fearing more the invasion of privacy from the state not the market."[98] The U.S. privacy regime has been described as "fragmented, ad hoc, and narrowly targeted to cover specific sectors and concerns."[99] While OMB oversees privacy for the federal agencies, there is no privacy oversight agency for the private sector.[100] Instead, the FTC has some oversight and limited enforcement powers for areas such as consumer credit information, but its predominant role is to educate consumers and support industry in developing and monitoring their corporate codes of conduct. Other agencies or regulatory bodies also exercise some limited oversight and enforcement power, which is often sector and issue-specific.[101] The theory supporting self-regulation is that privacy protection is in the economic interest of the companies themselves.[102]

---

96. *See* Shaffer, *supra* note 94, at 24. ("The vast majority of states lack omnibus privacy acts, and instead offer scattered statutes applying to specific sectors or concerns . . ."); *see generally* ROBERT ELLIS SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (2002).

97. Bart Lazar, *Security Breach Responses – As Important and Difficult as Ever*, SEYFARTH SHAW: TRADING SECRETS (June 8, 2018), https://www.tradesecretslaw.com/2018/06/articles/cybersecurity/security-breach-responses-as-important-and-difficult-as-ever/.

98. William J. Long & Marc Pang Quek, *Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise*, 9 J. EUR. PUB. POL'Y. 325, 331 (2002).

99. Shaffer, *supra* note 94, at 22; *see also* Long & Quek, *supra* note 98, at 331.

100. *See* Shaffer, *supra* note 94, at 23; *see also* Long & Quek, *supra* note 98, at 332.

101. Eric G. Orlinsky et al., *Cybersecurity: A Legal Perspective*, 47 MD. B. J. 33, 36 (2014). ("While there is no general federal duty to protect personal data, there are more than 50 federal statutes addressing cybersecurity in some form. Statutes range from routine disclosure mandates to affirmative obligations to prevent breaches. . .For example, the Securities and Exchange Commission now requires public companies to make certain disclosures about cyber threats and risks to investors.").

102. *See generally* Peter P. Swire, Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in Chapter 1: Theory of Markets and Privacy, National

In both the public and private spheres, privacy rights are affirmed so long as an individual is informed, or in some cases given an opportunity to consent to, how his personal information would be collected, used, and shared. But while this concept of privacy protection made sense in the age of newspapers, television, and analog internet, in the age of big data, artificial intelligence, and the internet-of-things, the validity of this privacy scheme completely disintegrates.

With greater portions of our social, economic, and personal lives tied to information technology, consumers no longer have the opportunity to understand – let alone decide – how their personal information is collected, shared, and used.[103] In the digital age, individuals are forced to interact with a wide range of media that compels them to "readily and willingly exchange information under conditions and in circumstances that they do not adequately understand."[104] Consumers are overloaded with information and "lack the time and attention required to control their privacy."[105] As one scholar states, individuals have become only passively attentive to how their personal information is collected and used.[106] In effect, society is increasingly "surrendering" information to technology.[107]

Surrendering to technology is both a cause and an effect of the increasing loss of privacy. As greater portions of life become computer-mediated, there is an increasing lack of attention to how much of our personal information is surrendered to technology in consideration for performing the simplest routines. Likewise, as we willingly expose more of our personal details and lives to the internet, whether for increased efficiency or fulfillment of our lives, we increasingly trust, sometimes with little forethought, the technology to safeguard this information.[108]

> Judgments about technology have been made on narrow grounds, paying attention to such matters as whether a new device serves a particular need, performs more efficiently than its predecessor, makes a profit, or provides a convenient service. Only later does the broader significance of the choice become clear, typically as a series of surprising "side effects" or "secondary consequences."[109]

Paul Scharre, who co-authored a think tank report on artificial intelligence, stated, "[r]ight now, the one saving grace is that the sheer volume of information

---

Telecommunications and Information Administration, (n.d.), https://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy#nav.

103. *See* BOUSKILL, CHONDE & WELSER, *supra* note 14, at 5 ("Technology is becoming faster, flashier, and more compact, seemingly slipping into our pockets without much deliberation.").

104. Walker, *supra* note 89, at 145.

105. *Id*. at 144.

106. *See id*. at 144–158.

107. *Id*.

108. *Id*.

109. WINNER, *supra* note 62, at 9.

[about a person] makes it very difficult to do anything. . .at scale."[110] However, an emerging feature of artificial intelligence and big data analytics is the capability to "reassemble the data trail" and use it to target individuals.[111] "Big data analytics has the power to provide insights about people that are far and above what they know about themselves."[112] The data-information-knowledge-wisdom (DIKW) hierarchy, which is widely used in information science, can be useful to depict this point.

At the bottom of this hierarchy is the raw data or information that has yet to be processed, analyzed, or connected to other data.[113] Information, which is the next level up, refers to data that has undergone some degree of processing[114] – for example, calculating the number of users that have clicked on a particular website. At the information level, data is no longer "raw." Some analysis has occurred, whether adding up the data points into a sum or identifying characteristics, anomalies, or patterns from raw data. Moving upwards, knowledge denotes a higher degree of understanding of the interrelationships between data.[115] For example, knowledge would involve the ability to connect data dispersed between different information categories in order to build profiles of users. Wisdom reflects the highest level of this hierarchy, in which information and knowledge correspond to a more granular understanding of people to the point that the observer can begin to know more about the individual profiles, habits, and interests than the individuals themselves would understand.[116]

Organizations, including the U.S. government, are unprepared for an information environment[117] where observing entities – both human and artificial – can achieve "wisdom" on not only large populations but each individual in these populations.[118] When organizations think about privacy, they typically focus on the

110. Kaveh Waddell, *Report: The U.S. is Unprepared for the AI Future*, AXIOS (July 11, 2018), https://www.axios.com/the-us-isnt-ready-for-the-ai-future-96649a76-1027-43ba-ae27-e24cb57dd194.html.

111. *Id.*

112. John Weathington, *Big Data Privacy Is a Bigger Issue Than You Think*, TECH REPUBLIC (Feb. 17, 2017), https://www.techrepublic.com/article/big-data-privacy-is-a-bigger-issue-than-you-think/.

113. *Id.*

114. *Id.*

115. *Id.*

116. *Id.*

117. *See* U.S. DEP'T OF DEF., DOD STRATEGY FOR OPERATING IN THE INFORMATION ENVIRONMENT 3 (2016) (defining "Information Environment" as the "aggregate of individuals, organizations, and systems that collect, disseminate, or act on information.") (citation omitted).

118. *See generally IBM Study: Organizations Unprepared to Tackle Next Wave of Technology Trends*, IBM NEWS ROOM (May 19, 2014), http://www-03.ibm.com/press/us/en/pressrelease/43946.wss (according to a study by IBM, less than 10% of organizations surveyed in 18 countries and 19 industries say their existing information technology infrastructure is fully prepared for the proliferation of mobile devices, social media, data analytics and cloud computing); *see also* Rajiv Leventhal, *Report: Feds Say Big Data Will Improve Population Health Management*, HEALTHCARE INFORMATICS (Mar. 24, 2014), https://www.healthcare-informatics.com/news-item/report-feds-say-big-data-will-improve-population-health-management (The report, "The Big Data Cure," published by MeriTalk, a public-private partnership, surveyed federal executives focused on healthcare and healthcare research. The report found that "[l]ess than one in five says their agency is very prepared to work with big data. . .[f]ew have

level of data.[119] Sensitive data, in its raw form, like a bank account or Social Security number, have been the focal point for protection because linking a person to his or her Social Security number opens up a host of potential ways that the person can be harmed or even have their identity stolen. Little attention has been given to addressing the possibility that a person's most sensitive personal information could be exposed by leveraging otherwise innocuous or anonymous data.[120]

This focus on data as the litmus test for the protection of privacy has made its way into all parts of the U.S. privacy regime under the theory of anonymization. Anonymization is the theory that if information cannot be directly associated with a particular individual, then the particular person's identity can be deemed anonymous and his or her privacy rights are protected. The theory is embraced both in industry and the government.[121]

Taking an example from the U.S. code, under the Drivers Privacy Protection Act, a state's department of motor vehicles and its employees are prohibited from disclosing "personal information" to any third persons except under very restricted circumstances.[122] The Act defines personal information as an individual's photograph, Social Security number, and medical information, among other very specific fields.[123] Highly restricted personal information – which requires an individual's express consent for disclosure – is defined as an "individual's photograph or image, Social Security number, [and] medical or disability information."[124] Information such as one's zip code or gender do not qualify as directly traceable to a single person; therefore, they do not trigger any obligations under the Act.

Anonymization coincides with a separate but similar assumption that one's personal information can still be protected even when releasing business profile information such as official duties, position, and work history. Under this theory, it is assumed that one would not be able to use business profile information to identify more personal details on an individual.

Unless an exemption applies, under the Freedom of Information Act, federal agencies are required to disclose, upon request, information on a particular person's official duties and other background information. For example, upon receipt of a proper FOIA request for information on a DoD civilian employee or military

---

invested in IT systems/solutions to optimize data processing (34 percent), trained IT professionals to manage and analyze big data (29 percent), or educated senior management on big data issues (29 percent).").

119. Weathington, *supra* note 112.

120. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1706 (2010) ("For decades, technologists have believed that they could robustly protect people's privacy by making small changes to their data.").

121. *Id.* ("[R]egulators and technologists have promised privacy to users, and in turn, privacy is what users have come to expect. Today, anonymization is ubiquitous.").

122. Prohibition on release and use of certain personal information from State motor vehicle records, 18 U.S.C. § 2721 (2000).

123. *Id.* § 2725(3).

124. *Id.* § 2725(4).

service member, DoD normally discloses the name, present and past positions, rank or grade, present and past duty stations, and office and duty telephone numbers.[125] For service members, DoD also normally discloses their home of record and official photo, in addition to other information.[126] DoD does not, however, release entire lists of persons,[127] nor would DoD release any information on persons when they are assigned, detailed, or employed to certain intelligence agencies[128] or any overseas, sensitive, or routinely deployable unit.[129] Since the September 11th terrorist attacks, DoD has also taken additional measures to restrict the release of names of employees or service members under the grade or rank of director or colonel; however, this policy is routinely overwritten by the circumstances of the request and the nature of the records being requested.[130]

With the ubiquity of information and the constant accumulation of new data tied to individuals, seemingly innocuous information presents incredible risks to a person's privacy.

In a landmark study based on 1990 U.S. census data, 87 percent of the U.S. population can be identified by simply knowing the gender, zip code, and the full date of birth.[131] The evidence from this study pointed to the fact that the practice of "de-identifying data" and other practices of random information generalization are "not sufficient to render data anonymous" because combinations of other different data fields can be used to re-identify this data.[132] Using census data from 2000, researchers were able to re-confirm the findings from the 1990 census, although reaching a somewhat lower percentage – 67 percent of the U.S. population.[133]

---

125. U.S. DEP'T OF DEF., DIR. 5400.11-R, DOD PRIVACY PROGRAM paras. C4.2.2.5.1-C4.2.2.5.2 (2007) ("C4.2.2.5.2. Military Members . . . [T]he following items of personal information regarding individual military members normally may be disclosed without a clearly unwarranted invasion of their personal privacy: C4.2.2.5.2.1.1. Full name . . . Rank . . . Date of rank . . . Gross salary . . . Past duty assignments . . . Present duty assignment . . . Future assignments that are officially established . . . Office or duty telephone numbers . . . Source of commission . . . Promotion sequence number . . . Awards and decorations . . . Attendance at professional military schools . . . Duty status at any given time . . . Home of record (identification of the state only) . . . Length of military service . . . Basic Pay Entry Date . . . Official Photo.").

126. *Id.*

127. *Id.* at para. C4.2.2.7.

128. *Id.* at para. C4.2.2.6 (naming specifically, the National Security Agency, the Defense Intelligence Agency, the National Reconnaissance Office, and the National Geospatial-Intelligence Agency).

129. *Id.*

130. *See* U.S. DEP'T OF DEF., O1-CORR-101, WITHHOLDING OF PERSONALLY IDENTIFYING INFORMATION UNDER THE FREEDOM OF INFORMATION ACT (FOIA) (2001) ("Ordinarily names of DoD personnel, other than lists of names, mentioned in documents that are releasable under the FOIA should not be withheld, but in special circumstances where the release of a particular name would raise substantial security or privacy concerns, such a name may be withheld.").

131. Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* 17 (Carnegie Mellon Univ., Data Privacy Working Paper No. 3, 2000), https://dataprivacylab.org/projects/identifiability/paper1.pdf.

132. *Id.* at 2.

133. Philippe Golle, *Revisiting the Uniqueness of Simple Demographics in the US Population*, PALO ALTO RESEARCH CENTER (2006).

These studies' findings demonstrate how easily people can be re-identified through only a few basic data fields. The examples of America Online and Netflix's data releases underscore this point.

In 2006, America Online (AOL) publicly posted the search log for 650,000 users of its search engine, which reflected approximately 36 million individual searches.[134] The public release was intended to be a gesture in the spirit of academic research. Without user names, it was believed that the data was completely anonymous; however, shortly thereafter, the *New York Times* debunked the theory of anonymity by re-identifying one AOL searcher. Upon inquiry by the *New York Times*, 62-year old Thelma Arnold, a widow from Lilburn, Georgia, confirmed that she was AOL Searcher 4417749, who entered search terms relating to "numb fingers," "60 single men," and "dog that urinates on everything."[135]

In the same year as AOL's release of its search log, the movie rental company, Netflix, publicly released a log of approximately a hundred million records relating to the movie ratings of a half million of its users over a six-year period.[136] The company released the data as a part of a contest to improve its movie recommendations software. The release was considered "anonymous" because Netflix had removed personal usernames. The records would contain the name of the movie rated, the rating assigned, date of rating, and a unique user identifier to allow someone to track the ratings of each user over time.[137] Similar to the AOL example, however, privacy researchers used information from another publicly available database to triangulate the identity of "anonymous" Netflix customers.[138]

IV. PERSONAL INFORMATION AS AN ATTACK VECTOR

The ability to reach the most sensitive information on people and triangulate it to individuals increases by the day. Leveraging the ever-expanding data pool, data firms are increasingly harvesting and trading personal data as a commodity. Governments and non-governmental entities, in turn, are increasingly leveraging the efficiencies of big data, artificial intelligence, and other emerging technologies to increase efficiency, influence, power, and control.[139] These data pools can cover a limitless spectrum of personal information, all of which present

134. Paul Boutin, *You Are What You Search*, SLATE (Aug. 11, 2006), https://slate.com/technology/2006/08/the-seven-ways-that-people-search-the-web.html.

135. *See* Ohm, *supra* note 120, at 1718; *see also* Boutin, *supra* note 134.

136. *See* Ohm, *supra* note 120, at 1720; *see also* Taylor Buley, *Netflix Settles Privacy Lawsuit, Cancels Prize Sequel*, FORBES (Mar. 12, 2010), https://www.forbes.com/sites/firewall/2010/03/12/netflix-settles-privacy-suit-cancels-netflix-prize-two-sequel/#3429c5f0951e.

137. Ohm, *supra* note 120, at 1720.

138. Buley, *supra* note 136 (discussing how privacy researchers Arvind Narayanan and Vitaly Shmatikov used comments from the "Internet Movie Database" to connect to anonymous users in the Netflix records release).

139. *See* Zoe Williams, *Algorithms Are Taking Over – And Woe Betide Anyone They Class as a 'Deadbeat'*, THE GUARDIAN (July 12, 2018), https://www.theguardian.com/world/commentisfree/2018/jul/12/algorithm-privacy-data-surveillance; *see also* Miranda Hall & Duncan McCann, *What's Your Score: How Discriminatory Algorithms Control Access and Opportunity*, NEW ECONOMICS FOUNDATION (July 10, 2018), https://neweconomics.org/2018/07/whats-your-score.

opportunities for new ways to hyper-personalize services and bring newfound efficiencies and ways to achieve social and personal fulfillment. However, with this emerging information world, there comes a darker side. As individuals trust greater portions of their lives to digital technology, creating ever richer databases, their personal information stands increasingly open to exploitation and attack by malevolent actors.

Over the past century, U.S. defense planning and assessments of strategic risk hinged on calculations of rival powers' capabilities and capacity to contest U.S. strategic objectives in a direct military engagement.[140] Globalization and technology, however, open up new opportunities and pathways for undermining U.S. strategic interests and countering U.S. advantages without direct military confrontation.[141] For defense and military strategists, this new environment is broadly encapsulated in the concept coined as the "gray zone."[142]

The gray zone is a broad concept to describe the universe of openings and opportunities for achieving strategic objectives through tactics, strategies, and maneuvers that are neither clearly in the domains of war nor peace.[143] U.S. competitors have learned to exploit the gray zone with a "mixture of capabilities and methods at the strategic, operational, and tactical levels of decision and action."[144] Using a "mosaic" of political, military, economic, and information domains,[145] U.S. competitors can identify and exploit gaps, seams, and vulnerabilities in the post-World War II order, leaving the United States and its allies off-balance, unprepared, or effectively without options that do not incur prohibitive costs. To date, the United States has failed to "come up with a coherent countervailing approach."[146]

U.S. "dominance in warfare has given adversaries... a strong motivation to adopt asymmetric methods," particularly in the information domain where our dependence on technology presents opportunities for exploitation.[147] Information warfare takes place below the level of armed conflict, encompassing a "range of military and government operations to protect and exploit the information

140. *See* JOINT CHIEFS OF STAFF, JOINT PUB. 2-01, JOINT AND NATIONAL INTELLIGENCE SUPPORT TO MILITARY OPERATIONS I-2 (2017); *see also* Nathan P. Freier et al., *Outplayed: Regaining Strategic Initiative in the Gray Zone*, U.S. ARMY WAR COLLEGE at 14 (June 2016), https://apps.dtic.mil/dtic/tr/fulltext/u2/1013807.pdf.

141. JOINT PUB. 2-01, *supra* note 140, at I-2.

142. *See generally* Freier et al., *supra* note 140.

143. *Id*. at 3.

144. *Id*. at 14.

145. *Id*.

146. *Id*. at xiii.

147. JOINT PUB. 2-01, *supra* note 140, at I-2; *see also* STEVEN METZ & DOUGLAS V. JOHNSON, ASYMMETRY AND U.S. MILITARY STRATEGY: DEFINITION, BACKGROUND, AND STRATEGIC CONCEPTS (2001) (discussing the history of the modern term); Guo-Woei Jinn, *China's Development of Asymmetric Warfare and the Security of Taiwan, Republic of China*, NAVAL POSTGRADUATE SCHOOL, Dec. 2004, at 14-17 (discussing "asymmetric warfare" both in U.S. and Chinese military doctrine); JOINT CHIEFS OF STAFF, JOINT VISION 2020: AMERICA'S MILITARY PREPARING FOR TOMORROW 73 (2000), https://apps.dtic.mil/dtic/tr/fulltext/u2/a526044.pdf ("[O]ur ever-increasing dependence on information processes, systems, and technologies adds potential vulnerabilities that must be defended.").

environment."[148] Information warfare can include tactics ranging from offensive methods such as disinformation, propaganda, and misinformation, to more defensive methods such as information assurance and information security.[149] "As cyberspace presents an easy, cost-effective method to communicate a message to large swaths of populations, much of present day information warfare takes place on the internet."[150]

Nowhere is this form of asymmetric, internet-driven, information warfare better illustrated than in the Russian activities surrounding the 2016 U.S. presidential election. The Russian activities surrounding the 2016 U.S. presidential election provide a poignant example of the confluence of asymmetric strategy, technology, and information warfare.[151]

According to a declassified version of a highly classified assessment by the U.S. Intelligence Community, Russia attempted to influence the U.S. presidential election through covert intelligence operations dedicated to obtaining and releasing sensitive information on U.S. persons.[152] In conjunction with this covert operation, Russia leveraged Russian government agencies, state-funded media, third-party intermediaries, and paid social media users to disparage U.S. presidential candidates deemed hostile to the Kremlin.[153]

The attack represented a multi-pronged, iterative strategy aimed at embarrassing and disrupting the Democratic National Committee (DNC) campaign for Hillary Clinton. Beginning as early as March 2016, units under the Main Intelligence Directorate of the General Staff (GRU) of the Russian Federation hacked employees and staff of the Clinton Campaign.[154] In July 2016, WikiLeaks, which was widely believed to be acting under Russian direction, released over 18,000 emails from the DNC to show the campaign's bias for and against its own candidates. The release led to the resignation of key DNC leaders and a flurry of controversy surrounding the presidential campaign to elect Hillary Clinton.[155] In October, WikiLeaks began releasing thousands of emails originating from the account of John D. Podesta, Mrs. Clinton's campaign manager, and in November,

148. CATHERINE A. THEOHARY, CONG. RESEARCH SERV., R45142, INFORMATION WARFARE: ISSUES FOR CONGRESS, Summary (2018).

149. *Id.*

150. *Id.*

151. *See* Media Ajir & Bethany Vailliant, *Russian Information Warfare: Implications for Deterrence Theory*, STRATEGIC STUD. Q. 83 (2018) ("[T]he evolution of military operations must include a sixth official dimension of warfare, psychological, overlapping but distinctly separate from cyber. . . The weaponization of information changes the application of deterrence, both within the cyber domain and in a psychological domain.").

152. NAT'L. INTELLIGENCE COUNCIL OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ICA 2017-01D, ASSESSING RUSSIAN ACTIVITIES & INTENTIONS IN RECENT U.S. ELECTIONS ii (2017); *see also* 1 ROBERT S. MUELLER, III, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION (2019).

153. NAT'L. INTELLIGENCE COUNCIL, *supra* note 152; MUELLER, *supra* note 152.

154. MUELLER, *supra*. note 152, at 36.

155. William Banks, *State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0*, 95 TEX. L. REV. 1487, 1487 (2017).

two days before the election, an additional batch of emails was released.[156] Former Democratic National Committee Chairperson, Debbie Wasserman Schultz, described the situation as one of "weaponiz[ing] information."[157]

Immediately after Election Day, the U.S. Intelligence Community determined that Russian intelligence was continuing to conduct a campaign specifically "targeting U.S. Government employees and individuals associated with U.S. think tanks and NGOs in national security, defense, and foreign policy fields."[158] Russia's attack on the presidential election represented one of the boldest efforts at influencing U.S. elections, and given its past practice and current efforts, the Intelligence Community assessed the situation as the "new normal" for our information world.[159]

V. THE "NEW NORMAL"

The current privacy regime has fallen well behind not only in understanding and regulation of this emerging landscape, but also planning, foresight, and response. The Russian activities surrounding the 2016 U.S. presidential election reflect only one example of how valuable our personal information can be to a foreign adversary. The following examples underscore this point and more importantly highlight how unprepared the United States is in the face of this new attack vector.

A. Sony Pictures Entertainment

In November 2014, a group of North Korea-linked hackers attacked employees of Sony Pictures Entertainment in retaliation for a proposed release of a Hollywood comedy film about a fictitious plan to assassinate the leader of North Korea.[160] The hackers initially targeted the company's executives to retaliate against the release of the film. They released a tranche of personal emails and company documents with the demand that Sony Pictures Entertainment cancel the proposed release or suffer additional harm.[161] The hackers, thereafter, continued to release personal information of employees and their dependents – including emails between employees, information about executive salaries, copies of unreleased films, and other information – all in what was a coordinated attack to change company policy with respect to a satirical film about North Korea's leader, Kim Jong Un.[162]

---

156. *Id.*

157. Amy Russo, *Ex-DNC Chair: Roger Stone 'Weaponized' Intel 'Stolen' by Putin*, HUFFINGTON POST (Jan. 27, 2019), https://www.huffingtonpost.com/entry/debbie-wasserman-schultz-roger-stone_us_5c4d7297e4b0287e5b8b7bf4 (describing the Ex-DNC Chair's comments in relation to the indictment of former unofficial Republican campaign advisor Roger Stone, who was indicted for false testimony before Congress, witness tampering, and obstruction of justice).

158. NAT'L. INTELLIGENCE COUNCIL, *supra* note 152, at 5.

159. *Id.*

160. *See* Criminal Complaint, United States. v. Park Jin Hyok, No. MJ-18-1479 (C.D. Cal. June 8, 2018), https://www.justice.gov/opa/press-release/file/1092091/download.

161. *Id.*

162. Eldar Haber, *The Cyber Civil War*, 44 HOFSTRA L. REV. 41, 41 (2018); Kim Zetter, *Sony Got Hacked Hard: What We Know and Don't Know So Far*, WIRED (Dec. 3, 2014), http://www.wired.com/2014/12/sony-hack-what-we-know.

The attack on Sony Pictures Entertainment is important in that it illustrates how attacks on personal information of key persons can be used to influence changes to an entity's operations, and it also illustrates the lack of planning and response strategies to this type of attack. Apart from the uniqueness of a state actor's attack on a corporate entity,[163] the attack was significant in that it resulted in the company's at least partial acquiescence to the North Korean hackers' principle demands. Ultimately, as a result of the attacks and subsequent threats of attacks on any theaters who released the film, Sony Pictures Entertainment decided to cancel the release to theaters.[164]

The attack also demonstrated the inadequacy of protection options. As a result of the breach of personal information, employees of Sony Pictures Entertainment were relegated to filing a class-action lawsuit against the company for failure to maintain "reasonable and adequate security measures" to protect their information.[165] Sony Pictures filed a motion to dismiss,[166] and while the judge was sympathetic to the plaintiffs' actual costs in credit monitoring and related services, he ultimately dismissed many of the non-monetary claims. The court found that the claims relating to future harms and lost time for dealing with the breach were too speculative.[167] Sony eventually settled the case for approximately $15 million in addition to a $2 million fund to help the employees protect themselves from identity theft.[168] Although the settlement may be seen as a partial victory for the plaintiffs, the court's dismissal of the plaintiffs' non-monetary losses associated with embarrassment and other "speculative" damages demonstrates how narrow the protections may be for individuals who are harmed by privacy breaches.

Ultimately, despite the far-reaching and public spectacle of the breach, the company did not have an ex-post mitigation plan and the employees were largely dependent on the courts to secure relief – a relief that was limited to what they could prove in monetary damages.[169]

---

163. *See* Amended Class Action Complaint, Corona v. Sony Pictures Entertainment, No. 2:14-CV-09600-RGK-SH (C.D. Cal. Mar. 2, 2015), ECF No. 43, https://www.krcomplexlit.com/ wp-content/uploads/2015/09/AmendedComplaint43030215.pdf.; *see also* Ellen Nakashima, *U.S. Attributes Cyberattack on Sony to North Korea*, WASH. POST. (Dec. 19, 2014), https://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702fa31ff4ae98e_story.html?utmterm=.7e0e0d272be1&noredirect=on.

164. Lawrence J. Trautman & Peter C. Ormerod, *WannaCry, Ransomware, and the Emerging Threat to Corporations*, 86 TENN. L. REV. 503, 526 (2019).

165. Josephine Wolff, *"An Epic Nightmare": What Came After the Sony Breach*, SLATE (Nov. 27, 2018), https://slate.com/technology/2018/11/north-korea-sony-pictures-hack-humiliation-response.html.

166. *See generally* Corona v. Sony Pictures Entertainment, Inc., Case No. 14-CV09600-RGK (Ex), (C.D. Cal. June 15, 2015), ECF No. 97, https://www.lieffcabraser.com/pdf/Sony-order-20150615.pdf (motion to dismiss granted in part).

167. Wolff, *supra* note 165.

168. *Id.*

169. *Id.*

B. Yahoo Email

In 2013, the web services provider Yahoo suffered a data breach in which the names, email addresses, and passwords of every user at the time were accessed by hackers believed to be affiliated with the Russian intelligence services.[170] The overall extent of the attack is believed to have reached over 3 billion users.[171] In a separate breach that occurred in 2014, approximately 500 million people were also exposed by Russian hackers.

Not long after the 2013 breach, the information collected from the attack was found to have been posted for sale on the dark web. According to one cybersecurity firm, the information was sold to three parties for $300,000 each; however, the data remains for sale on the black market.[172]

Though Yahoo is not the only web service provider to have been hacked, its breach was certainly the largest. An intelligence expert for the cybersecurity firm, InfoArmor, stated that his company had informed law enforcement agencies that the data contained information from employees in the Federal Bureau of Investigation, National Security Agency, the White House and officials of the United Kingdom.[173]

C. Starwood Guest Reservation Database

In 2018, Marriott International announced the discovery of a breach of its Starwood guest reservation database, in which the information on up to 383 million guests was accessed by hackers.[174] The company reported that the information included "some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation data, communication preferences, and encrypted payment card numbers."[175] The company believes that approximately 8.6 million unique payment card numbers were involved in the incident; however, the number of unexpired payment card numbers that could have been unencrypted is significantly lower based on the company's ongoing analysis of the breach.[176] In addition, the company believes that "approximately 5.25 million unique unencrypted passport numbers and approximately 20.3 million encrypted passport numbers" were stolen by the hackers.[177] Given the scope and methods used, the U.S. government believes, in its preliminary findings, that the hackers were

170. Nicole Perlroth, *All Three Billion Yahoo Accounts Were Affected by 2013 Attack*, N.Y. TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.

171. *Id.*

172. *Id.*

173. *Id.*

174. STARWOOD GUEST RESERVATION DATABASE SECURITY INCIDENT: MARRIOTT INTERNATIONAL (Mar. 4, 2019), https://perma.cc/2242-X7JU.

175. *Id.*

176. *Id.*

177. *Id.*

affiliated with the Chinese Ministry of State Security.[178]

The Marriott International data breach is significant as it illuminates the value of identifying people's travel habits, schedules, and passport data. As Michael Daly, cybersecurity chief technology officer for Raytheon Intelligence states,

> This is much more than a consumer data breach. When you think of this from an intelligence gathering standpoint, it is illuminating the patterns of life of global political and business leaders, including who they traveled with, when and where. That is incredibly efficient reconnaissance gathering and elevates this breach to a national security problem.[179]

D. Ransomware

In 2017, the WannaCry virus struck an estimated 300,000 computer systems with a ransomware attack.[180] The virus was particularly significant in that once a single machine was affected, the virus would spread automatically to all connected local area networks (LANs) and wide area networks (WANs) without user interaction.[181]

Similar to other ransomware viruses, once the WannaCry virus had infected a system, the victim's data would be encrypted and the victim would receive a ransom payment demand for data recovery.[182] The distinguishing feature of the WannaCry virus is its worm-like qualities, which accentuated its impact and spread around the globe.[183]

Ransomware is not a new problem, nor is it isolated to particular systems or regions of the world.[184] The FBI estimates that over 100,000 computers are

178. Doreen McCallister, *Chinese Hackers Are Likely Responsible for Marriott Data Breach, Reports Say*, NPR (Dec. 12, 2018), https://www.npr.org/2018/12/12/675983642/chinese-hackers-are-responsible-for-marriott-data-breach-reports-say; *see also* David E. Sanger et al., *Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing*, N.Y. TIMES (Dec. 11, 2018), https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.

179. David Volodzko, *Marriott Breach Exposes Far More than Just Data*, FORBES (Dec. 4, 2018), https://www.forbes.com/sites/davidvolodzko/2018/12/04/marriott-breach-exposes-far-more-than-just-data/#ef6b34762978. Patrick Clark, *Marriott's $13.6 Billion Starwood Deal Bought Security Risk*, BLOOMBERG (Nov. 20, 2018), https://www.bloomberg.com/news/articles/2018-11-30/marriott-s-13-6-billion-starwood-deal-also-bought-security-risk.

180. Calyptix, *supra* note 4; *cf.* Russell Goldman, *What We Know and Don't Know About the International Cyberattack*, N.Y. TIMES (May 12, 2017), https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html (claiming a smaller number of affected computers or 200,000).

181. Calyptix, *supra* note 4.

182. Dan Goodin, *An NSA-Derived Ransomware Worm Is Shutting Down Computers Worldwide*, ARS TECHNICA (May 12, 2017), https://arstechnica.com/security/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/.

183. *See id.*; *see also* Criminal Complaint, United States. v. Park Jin Hyok, *supra* note 160 (claiming North Korean hackers as the authors for the malware named "Wanna Cry 2.0").

184. Rod Rosenstein, Deputy Attorney General, Remarks at the 2017 North America Int'l Cyber Summit (Oct. 30, 2017), https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-

infected by ransomware per day around the world.[185] The software has hit all economic sectors as well as countless institutions and government systems. Its costs on the global economy are also expected to exponentially increase. By the end of 2019, ransomware is expected to attack a business every 14 seconds, and according to one cybersecurity firm, the damages to the world economy will rise to $11.5 billion in 2019 alone.[186]

The significance of ransomware is not only its significant financial impact on victims, but the potential for its increased access to targets through emerging technologies. As more functions, activities, and aspects of life become digitized and interconnected, the ability for ransomware to reach victims through these interconnected devices will increase. Bruce Schneier, a widely-respected expert on information technology and security, states:

> Everything is becoming a computer. Your microwave is a computer that makes things hot. Your refrigerator is a computer that keeps things cold. Your car and television, the traffic lights and signals in your city and our national power grid are all computers. This is the much-hyped Internet of Things (IoT). It's coming, and it's coming faster than you think. And as these devices connect to the Internet, they become vulnerable to ransomware and other computer threats.[187]

E. Office of Personnel Management Data Breach

Although the attack on the Office of Personnel Management (OPM) occurred earlier than the former cases, it is discussed as the final example because of its significance. Between 2014 and 2015, attackers exfiltrated personnel files of 4.2 million former and current government employees and security clearance background investigation information on 21.5 million individuals.[188] The breach and exfiltration of data included the entire spectrum of information one could expect to find in a background investigation or security clearance file, including fingerprint records of 5.6 million employees.[189]

The significance of the attack could not be understated. Joel Brenner, former NSA senior counsel stated, "This is crown jewels material. . . a gold mine for a

---

remarks-2017-north-american-international (discussing how "[a] few years ago, ransomware attacks were unsophisticated and haphazard[].").

185. *Id.*

186. Steve Morgan, *Ransomware Damage Costs Predicted to Hit $11.5B by 2019*, CSO (Nov. 20, 2017), https://www.csoonline.com/article/3237674/ransomware/ransomware-damage-costs-predicted-to-hit-115b-by-2019.html.

187. Bruce Schneier, *The Future of Ransomware*, SCHNEIER ON SECURITY (May 23, 2017), https://www.schneier.com/blog/archives/2017/05/the_future_of_r.html.

188. STAFF OF H. COMM. ON OVERSIGHT AND GOV'T REFORM, 114TH CONG., THE OPM DATA BREACH: HOW THE GOVERNMENT JEOPARDIZED OUR NATIONAL SECURITY FOR MORE THAN A GENERATION 5 (2016) ("Attackers had access to OPM's network. . .[and] US-CERT found malware (Hikit). . .on an OPM server since 2012."); *cf. id.* at viii (discussing how "[t]he exact details on how and when the attackers (X1, X2) gained entry and established a persistent presence in OPM's network are not entirely clear. . .due to sloppy cyber hygiene and inadequate security technologies.").

189. *Id.* at 13.

foreign intelligence service."[190] John Schindler, former NSA officer opined, "[w]e cannot undo this damage. What is done is done[,] and it will take decades to fix."[191] Finally, Michael Hayden, former director of the CIA, described OPM's data as "a treasure trove of information that is available to the Chinese until the people represented by the information age off. There's no fixing it."[192]

Apart from the fact that this data breach represented the "crown jewels" of national security data held by OPM, this breach is important for the fact that it illustrates the government's then over-reliance on perimeter defenses at the expense of seeing risks and threats from within. OPM's cybersecurity plans overemphasized the value of maintaining one's perimeter defenses, at the expense of defending against the attacker who, having compromised user credentials, could "utilize[] tactics to elevate their privilege[]. . . once inside the perimeter. . . [and] move throughout the OPM's network."[193]

VI. FUTURE ATTACK VECTORS & APPROACHES

Testifying before the Senate Armed Services Committee, Central Intelligence Agency Director Leon Panetta stated, "The next Pearl Harbor that we confront could very well be a cyberattack that cripples America's electrical grid and its security and financial systems."[194] Accordingly, the U.S. government has dedicated significant attention and resources to the cybersecurity of national military and critical infrastructure information and systems.[195] The United States prioritizes the security of information on our critical infrastructure, such as energy, water, and transportation, and we look at all government information systems as important components of our national security infrastructure. Personal information, on the other hand – which is everywhere and in nearly everything – is not considered within this category of critical national security assets.[196]

190. David Perera & Joseph Marks, *Newly Disclosed Hack Got "Crown Jewels,"* POLITICO (June 12, 2015), http://www.politico.com/story/2015/06/hackers-federal-employees-security-background-checks-118954.

191. *Ex-NSA Officer: OPM Hack Is Serious Breach of Worker Trust*, NPR (June 13, 2015), http://www.npr.org/2015/06/13/414149626/ex-nsa-officer-opm-hack-is-serious-breach-of-worker-trust.

192. Dan Verton, *Impact of OPM Breach Could Last More Than 40 years*, FEDSCOOP (July 10, 2015), http://fedscoop.com/opm-losses-a-40-year-problem-for-intelligence-community.

193. STAFF OF H. COMM. ON OVERSIGHT AND GOV'T REFORM, *supra* note 188, at 20.

194. Anna Mulrine, *CIA Chief Leon Panetta: The Next Pearl Harbor Could Be a Cyberattack*, CHRISTIAN SCIENCE MONITOR (June 9, 2011), http://www.csmonitor.com/USA/Military/2011/0609/CIA-chief-Leon-Panetta-The-next-Pearl-Harbor-could-be-a-cyberattack.

195. COUNCIL OF ECON. ADVISERS, EXEC. OFFICE OF THE PRESIDENT, THE COST OF MALICIOUS CYBER ACTIVITIES TO THE U.S. ECONOMY 3 (2018) (stating that according to the Office of the Director of National Intelligence (DNI), "cyber threats were the most important strategic threat facing the United States.").

196. *See, e.g.*, OFFICE OF THE PRESIDENT OF THE UNITED STATES, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA 8–10 (2018) (mentioning privacy – not in the context of operational security but – in the context of civil liberties, human rights, and fundamental freedoms).

Personal information, for all intents and purposes, represents a vulnerable "backdoor"[197] that the U.S. government, industry, or even individuals as it pertains to their own digital profiles, have not taken adequate notice of, let alone begun comprehensively addressing. Databanks holding troves of personal information continue to grow, and the technologies capable of exploiting these massive pools of information continue to increase in sophistication, efficiency, and effectiveness. As more of our life is connected and dependent on the digital world, and our connections to this world are hyper-personalized, the ability for a malevolent actor to wield destructive power over individual persons, entities, and governments through this backdoor will increase exponentially.

In many ways, as illustrated by the examples above, this situation has already come to fruition today.[198] However, despite the telltale signs of how vulnerable and valuable our personal information may be, American society has not prepared for a scenario in which the weaponization of our personal information becomes the doctrinal opening to, or force multiplier for, a digital Pearl Harbor.

Because personal information is tied to individuals as well as being ubiquitous to systems, organizations, and enterprises, it is important to consider the different ways in which personal information can obtain operational value.[199]

A malevolent adversary could be surgical in its attack, targeting key persons in the same way as was seen during the Russian intelligence services' efforts against the Democratic candidate for president. On the other hand, if the targeting aperture is widened, attacks on personal information could include the targeting of not necessarily key leaders, but key units, teams, or parts of an organization – for example, targeting an entire team of persons that may be critical to a specific organizational function or mission.

In the age of big data, artificial intelligence, and the internet-of-things, attack surfaces do not necessarily have to be narrow or surgical in nature. Blanket targeting of an entire organization or enterprise population is feasible, particularly if the attack is part of a coordinated campaign to impact an organization, enterprise or country's capacity or capabilities. An example of such an attack could be a ransomware attack on an entire hospital facility or municipality, which has occurred

197. *See* Criminal Complaint, United States v. Park Jin Hyok, *supra* note 160, at 7 ("A 'backdoor' is a type of malware that allows a hacker to maintain access to a compromised computer after a computer is first compromised." In many ways, personal information can be construed as both a means and an end to compromise systems, organizations, and enterprises. Personal information can be both a vehicle for initiating access or an alternative "backdoor" to maintain access should alternative cyber tools into these targets become detected or disrupted.).

198. PWC, MANAGING CYBER RISKS IN AN INTERCONNECTED WORLD: KEY FINDINGS FROM THE GLOBAL STATE OF INFORMATION SECURITY SURVEY 2015 16 (2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (describing how in 2014, there was an "86% increase in respondents who say they have been compromised by nation-states.").

199. *See* JOINT CHIEFS OF STAFF, JOINT PUB. 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 174 (2016) (defining operation as "1. [a] sequence of tactical actions with a common purpose or unifying theme. . . . 2. A military action or the carrying out of a strategic, operational, tactical, service, training, or administrative military mission.").

on a number of occasions already.[200] Another example of this scenario may be an attack that is specific to logisticians, mobilization planners, or contractors responsible for supporting movement of a particular unit from the mobilization station to the port of embarkation.

As stated in the Defense Transportation Regulation, "[m]obilization activities are supported principally by intra-Continental United States (CONUS) air, rail, highway, pipeline, port facilities, and inland waterway assets of commercial firms."[201] An intelligent adversary would identify these firms and the key staff associated with the strategic hubs for mobilization. Triangulating their identity from multiple data sources, an adversary could then choose to attack a select number of personnel as a demonstration of force to sow fear, mistrust, and distraction in the target population. An enemy could attack wireless access points using de-authentication, use of an evil port, or domain name system (DNS) spoofing to undermine any and all digital technology used by the victims that are not within government servers.

Attacks on specific websites used by target populations have been described as "watering hole" attacks.[202] In these attacks, hackers will identify a website that is frequented by their target population. Once identified, the website will be compromised or infected with some form of malicious software that is then passed onto visitors to the website. In 2015, an aerospace company's website was infected with an Adobe Flash virus that gave the hackers control over the information systems of visitors to the website.[203]

Alternatively, or in addition, hackers could attack smart devices associated with the victims to harass, harm, and wreak financial ruin. Although higher-profile attacks would trigger law enforcement or national security responses, it is questionable as to how individual victims would alert their organizations of such an attack or how the organizations themselves would be able to respond. It is likely that organizations would struggle with mitigating the impact on the mission or helping individuals salvage their personal affairs, particularly because there is no breach response plan that anticipates a distributed attack on personal information residing on systems external to DoD or government networks.

Attacks on personal information do not necessarily have to be direct. In other words, an organization could be attacked directly by breaching its pay, health, and personnel records; however, a malevolent actor could also be less direct by attacking third parties, such as contractors, dependents, or auxiliary support systems. Indirect attacks, such as an attack on the schools, banks, medical facilities,

200. *See* Trautman & Ormerod, *supra* note 164, at 23.

201. U.S. DEP'T OF DEF., DEFENSE TRANSPORTATION REGULATION – PART III MOBILITY III-302-1 (2017).

202. P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 43–44 (2014).

203. Danielle Correa, *Watering Hole Attack on Aerospace Firm Leveraged Flash 0day*, SC MEDIA (July 21, 2015), https://www.scmagazineuk.com/watering-hole-attack-aerospace-firm-leveraged-flash-0day/article/1479949.

and other social and municipal institutions supporting an organization's employees and their families could distract, if not undermine, the organization's mission effectiveness. Indirect attacks could include attacks on an organization's reputation through disinformation and the release of personal information of key persons. This approach was demonstrated in the attack on Sony Pictures Entertainment, in which the embarrassment of key persons in the organization was used to pressure certain changes in the organization's behavior, such as cancellation of a film's release. In effect, an adversary may be able to achieve a desired end-state more effectively through indirect targeting because such an attack would obscure the strategic goal, muddle attribution, or exploit "gray" areas in the law.

Attacks on personal information are not associated with any particular level of war. Personal information can be wielded to achieve tactical, operational, and strategic objectives. Accordingly, an attack on personal information could be high or low profile. In other words, an attacker may elect to assume a low profile for long term strategic value. By avoiding detection, an adversary would have a better chance of leveraging a target's institutional norms and behaviors to accentuate impact and achieve his or her desired end-state. For example, a hostile actor could target a key leader – releasing portions of personal information that is riddled with disinformation that triggers adverse organizational scrutiny, investigation, and repercussions for that individual. It could take weeks, if not months, before the disinformation could be distinguished and confidence in the individual restored. Alternatively, a higher profile action would invite a greater probability of a law enforcement or military response, which is what partially occurred with the Russian attacks on the Democratic National Committee.

A hostile actor can also adjust the gravity of the desired effect – for example, to create kinetic or non-kinetic effects. Although attacks on personal information can be exceptionally harmful to individual persons, as well as "destructive" to the finances and reputation of organizations, such attacks do not ordinarily meet the definition of a "destructive attack" under international law. In the wake of the attacks on Sony Pictures Entertainment, U.S. administration officials stated the attack "did not meet the traditional definition of a 'destructive attack' under international law, which involves death, injury, or damage or destruction of physical objects, such as computers."[204]

The International Group of Experts responsible for the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* noted that although the right to be free from arbitrary interference with one's privacy is part of customary international law, the "precise scope [of the right] is unsettled," and the right to privacy "has not yet crystallised into a customary norm."[205]

204. Nakashima, *supra* note 163.

205. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 189 (Michael N. Schmitt ed., 2d. 2017).

Thus, in many ways, most attacks on personal information would appear to be "non-kinetic" on their face. However, given the increasing use of the internet-of-things, it is feasible to see opportunities in which a hostile actor could use personal information as an entryway to devices that wreak physical destruction on a graduated scale.

For example, on the low end of the scale, attackers could hack into smart devices, such as a thermostat, to cause property damage.[206] A victim could receive a message on the smartphone application connected to the device demanding a ransom in exchange for initiating or continuing an attack.[207] Hackers have already demonstrated their ability to attack home cameras to take pictures and harass victims,[208] and researchers predict it is only a matter of time before "people get messages on their car screens saying that the engine has been disabled and it will cost $200 in bitcoin to turn it back on."[209] On the higher end of destruction, hackers could plausibly hack into one's medical devices, like a heart defibrillator or autonomous technology that exposes the victim to physical danger.[210]

Ultimately, although past attacks on personal information are instructive, it is important to consider them as merely signposts to what will be possible in the future. As the wealth of personal information on each of us grows, and technology increases, one can expect more novel operational and strategic approaches to this emerging facet of asymmetric, information warfare. The following vignettes are offered to provide some insights into this future landscape.

A. Vignette 1. Espionage, Counterintelligence, and Statecraft

Using information gleaned from the exploitation of the Starwood Guest Reservation breach, OPM's data breach, Yahoo, or any number of other social media, email, and other internet service breaches, malevolent actors could prevent, mitigate, or neutralize actions by U.S. intelligence agencies through the simple triangulation of data that allows for the identification of covert officers and agents. The scenario is not futuristic, and it is in fact occurring today.[211]

B. Vignette 2. Influence Operations

Similar to the operational effects on Sony Pictures Entertainment, personal information can be weaponized to influence individual and organizational behavior.

206. Schneier, *supra* note 187 (describing how researchers could hack into thermostats and adjust temperatures).

207. *See id.* (describing screenless thermostats).

208. Kristine Solomon, *Hackers Watched, Taunted Family Through Home Security Cameras: 'We Were Really Vulnerable'*, YAHOO (Jan. 24, 2019), https://www.yahoo.com/lifestyle/family-discovers-watched-hackers-home-security-cameras-really-vulnerable-202714623.html.

209. Schneier, *supra* note 187.

210. *Id.*

211. *See, e.g.*, Lisa Brownlee, *Report: Chinese Hackers Used OPM Data to Steal U.S. Military Intel; 'Significant Risk to U.S. Military'*, FORBES (Sept. 19, 2015), https://www.forbes.com/sites/lisabrownlee/2015/09/19/report-chinese-hackers-used-opm-data-to-steal-us-military-intel-significant-risk-to-us-military/#324f2fa96829 (discussing a cybersecurity firm's assessment that data from OPM's data breach was used by Chinese hackers to target defense contractors).

Using the risk of personal embarrassment as a pressure point, a hostile actor could influence a key leader's actions in an organization's strategic decision-point. Influence operations can also be used to harm the reputation of businesses or organizations to diminish the valuation of their "goodwill" assets or their prospects in a future market.[212] Attacking an organization's "soft power" can be an indirect way of achieving a desired end-state without triggering a heavy response.

A hostile actor can distract an organization in the execution of its mission through non-kinetic actions targeting an organization's employees and their dependents. Attacks on the family members of key employees through their smart devices or social media would increase stress to the force and create a burden on the organization to devote resources for mitigation, prevention, and response. A sophisticated adversary would not likely have to attack an entire unit or a large percentage of an organization to achieve the desired effect of sowing fear and mistrust about the organization's ability to protect its employees and families. Random targeting of a few key (or low-level) officials' dependents would likely lead to a ripple effect in heightened fear and precautions by the rest of the organization, which would increase stress, divert resources, and ultimately create new factors that the organization may not have considered, let alone planned for, in the execution of a mission or functional responsibility.

C. Vignette 3. Preparing the Battlespace

On a higher order of battle, personal information can be leveraged to prepare the battlespace by attacking military units (and their dependents) who are deploying to a theater of operations. Less direct or kinetic options could include the targeting of industry partners or other auxiliary support whose personal information may be easily exploited.[213] Persons identified as traveling to, working for, or associated with Mobilization Force Generating Installations, ports of embarkation, and disembarkation could serve as notional targeting criteria. A unit with a notice of sourcing could find members' personal information exploited to distract, undermine, or diminish an organization's ramp-up to war, and a sophisticated adversary would likely consider industry partners and auxiliary support as valuable targets for purposes of achieving an operational or strategic end-state of at least stressed, if not seriously hampered, mobilization timelines.[214]

---

212. *See generally* MUELLER, *supra* note 152 (describing the GRU's hacking of the Clinton Campaign and subsequent release of compromising material); *id*. at 41 ("The GRU released through dcleaks.com thousands of documents, including personal identifying and financial information, internal correspondence related to the Clinton Campaign and prior political jobs, and fundraising files and information.").

213. *See, e.g*., Criminal Complaint, United States v. Park Jin Hyok, *supra* note 160, at 4 (describing how the subjects of the North Korean cyber hacking organization responsible for attacking Sony Pictures Entertainment have also "targeted – and continue to target – other victims and sectors, including U.S. defense contractors, university faculty, technology companies, virtual currency exchanges, and U.S. electric utilities.").

214. *See, e.g*., Sebastian Bay et al., *The Current Digital Arena and Its Risks to Serving Military Personnel, in* RESPONDING TO COGNITIVE SECURITY CHALLENGES 7, 16 (Anna Reynolds & Giorgio Bertolin eds., 2019) (discussing how an adversary can leverage personal information gleaned from the

Major General Joseph Whitlock, writing for the Army Strategic Education Program, stated, "The United States is running a high risk that it may lose in a major theater war because it cannot mobilize and deploy the Army quickly enough."[215] When it comes to fighting a high-end war in the modern era, the Army must be prepared to "essentially call for up to five times as many reserve component units to mobilize in half the time that the nation has required in the post-9/11 era."[216] U.S. adversaries have taken consideration of this circumstance and re-oriented their strategy toward achieving military objectives at a lightning-fast pace to effectively deprive the United States of any options but to accept the new status quo.[217] On the opposite end of the spectrum, if an adversary could add friction and distractions to the U.S. military's mobilization and deployment timelines, then it can increase the timeline for which its military forces can secure operational objectives and maximize the competitive advantage when U.S. forces arrive.

Attacks on personal information during the initial period of war (IPW) would also align with some of our adversaries' operational doctrine. "Many Russian analysts believe the IPW will be a decisive element in any new conflict due to the ability of cyber methods to destroy infrastructure or command and control assets surreptitiously and with speed."[218]

Chinese military doctrine, in particular, has demonstrated an affinity for using information war as a "preemption weapon," rather than as a "battlefield force multiplier."[219] To defeat a more powerful adversary, one Chinese military theorist stated:

> We should zero in on the hubs and other crucial links in the system that moves enemy troops as well as the war-making machine, such as harbours, airports, means of transportation, battlefield installations, and the communications, command and control and information systems.[220]

---

social media of U.S. service members deployed in theater to compromise unit plans and locations, and even influence individual service members' conduct of their mission); *see also* Tara Copp, *NATO Troops Got Catfished and Honeypotted on Social Media, Revealing Serious Vulnerabilities*, MILITARY TIMES (Feb. 20, 2019), https://www.militarytimes.com/news/your-military/2019/02/20/nato-troops-got-catfished-honeypotted-and-revealed-how-vulnerable-they-are/.

215. Joseph Whitlock, *The Army's Mobilization Problem*, UNITED STATES ARMY WAR COLLEGE WAR ROOM (Oct. 13, 2017), https://warroom.armywarcollege.edu/articles/armys-mobilization-problem/.

216. *Id.*

217. *Id.*

218. TIMOTHY THOMAS, FOREIGN MILITARY STUDIES OFFICE, THINKING LIKE A RUSSIAN OFFICER: BASIC FACTORS AND CONTEMPORARY THINKING ON THE NATURE OF WAR 2 (2016); *see generally* Timothy Thomas, *Russian Military Thought: Concepts and Elements*, MITRE (2019), https://www.mitre.org/sites/default/files/publications/pr-19-1004-russian-military-thought-concepts-elements.pdf.

219. *See* James Mulvenon, *The PLA and Information Warfare, in* THE PEOPLE'S LIBERATION ARMY IN THE INFORMATION AGE 175, 183 (James C. Mulvenon & Richard H. Yang ed., 1999), https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF145/CF145.chap9.pdf.

220. Lu Linzhi, *Preemptive Strikes Crucial in Limited High-Tech Wars*, JIEFANGJUN BAO 6, FTS19960214000033 (Feb. 14, 1996).

D. Vignette 4. Attacks on Personal Information as a Force Multiplier in War

On the highest order of war, the personal information of key members of a deploying unit or government agency would be exposed to direct, kinetic attack. While a universe of circumstances – including legal and political considerations – would shape an adversary's strategy, approaches, and tactics, one could anticipate that, in the lessening of peace-time constraints, a soldier's participation in a battlespace could be justification for the targeting of his digital persona in all its facets. In such a scenario, his bank accounts could be legitimately emptied and all aspects of his digital persona subject to attack. Disinformation could be mingled with elements of his digital persona to maximize propaganda value, and his "home life" could be targeted.

The Geneva Conventions require that medical and religious personnel, medical units, and medical transports must be respected and protected, which means that they must not be made the object of attack.[221] However, it is unclear whether an adversary could – or would be willing to – target the medical information of deployed personnel, contractors, and auxiliaries who materially participate in a conflict. Altering or deleting medical, personnel, or pay records of war fighters and persons contributing to the war effort might be deemed a reasonable action in the midst of war in this new information landscape. Moreover, given the increasing use of mobile technology, the attack surface for identifying vulnerable entry points to the medical information of government personnel and service members is increasing.[222] Likewise, if one targets the industrial support to a war effort, then the personal information of industry and commercial partners could be subject to attack.

VII. RECOMMENDATIONS

The concept of the privacy of personal information has always been closely connected to the information environment at the time, and it was when this environment changed in a significant way that unexpected problems arose within the prevailing conception of privacy. The modern concept of privacy emerged with the rapid growth of newspapers and print media in the United States. The precepts of this early paradigm of privacy can be discerned from Warren and Brandeis' law review article, in which they argued for the protection of an individual's intangible, emotional self in the face of technology and enterprises that encroached upon the personal lives of people.[223]

---

221. *See* TALLINN MANUAL, *supra* note 205, at 515 (discussing medical computers, computer networks, and data).

222. *See generally* Chris Balcik, *DoD Is Doubling Down on Mobile Endpoint Security*, SAMSUNG INSIGHTS (Jan. 9, 2019), https://insights.samsung.com/2019/01/09/dod-is-doubling-down-on-mobile-endpoint-security/; Aubrey Merchant-Dest, *Perimeter Defense Won't Work for DoD in the Era of the Cloud*, FIFTH DOMAIN (May 31, 2018), https://www.fifthdomain.com/opinion/2018/05/31/perimeter-defense-wont-work-for-dod-in-the-era-of-the-cloud/.

223. Warren & Brandeis, *supra* note 7, at 196.

The advent of data processing and early computers, as well as the rise of the administrative state, challenged this paradigm of privacy because an individual's emotional self was not the only sense of "self" that required protection. With the rise of the administrative state and the corresponding and complementary advance of analog information technology,[224] an "analog self" emerged. Encapsulated within the mosaic of different records held by industry and principally government, people could face unwarranted invasions of their privacy that were not adequately addressed under law. A "crisis" occurred in the prevailing notions of privacy.[225] Because of the deluge of stories on actual and alleged government surveillance activities, the crisis appeared to be most pronounced in the government sector. As one U.S. senator stated,

> If we have learned anything in this last year of Watergate, it is that there must be limits upon what the Government can know about each of its citizens. Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.[226]

Even though big industry and the commercial sector were part of this mosaic of record-keeping institutions, the focal point for change was centered on the federal government – because of the size of the federal administrative state and its impact on citizens, as well as government improprieties that fed a public mistrust of government. In these circumstances, the Privacy Act of 1974 focused exclusively on the federal government's privacy responsibilities, and only various slices of the private sector, such as educational and financial services, would come under a limited form of federal privacy law.[227]

Since the passage of the Privacy Act, the paradigm for privacy within the federal government has been adjusted to meet the steady advances in information technology. From the Computer Matching and Privacy Protection Act,[228] E-Government Act,[229] and FISMA,[230] to the litany of OMB memoranda and

---

224. *See generally supra* Part I.

225. *See generally* SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., *supra* note 17.

226. Sen. Sam J. Ervin, Jr., *Introductory Remarks, on S. 3418*, *in* LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974 4 (U.S. Gov't Printing Office, 1976).

227. *See, e.g.*, Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2013) (regulating the accessibility of student records); Right to Financial Privacy Act of 1978, 29 U.S.C. §§ 3401–22 (2011) (requiring government officials to obtain a warrant or subpoena to access financial information); Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (provides access to credit records and restricts the manner in which they are disclosed).

228. Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100–503, 102 Stat. 2507 (codified as amended at 5 U.S.C. § 552a (1988).

229. E-Government Act of 2002, Pub. L. No. 107–347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3601).

circulars, the U.S. government has adjusted and included additional concepts to the fundamentals of the Privacy Act of 1974. Concepts such as privacy impact assessments and computer matching agreements bolstered the government's mechanisms for holding its executive branch organizations and officials accountable. In addition, new positions and processes were created to build privacy within organizational activities and decision-making. Senior agency officials for privacy were assigned responsibility for ensuring organizations comply with privacy requirements, and NIST integrated privacy controls within its security standards for federal information systems and organizations.

In the private sector, the paradigm of privacy was also adjusted to accommodate greater government oversight and regulation in the interest of protecting particularly vulnerable populations, sensitive data fields, or transactions that could significantly impact an individual's physical or financial well-being. To a very limited extent, industry has also exercised some degree of self-regulation in response to market forces and in anticipation of judicially-imposed remedies to plaintiff class actions.

The information environment that compelled the passage of the Privacy Act and its corollary laws and amendments, however, has evolved significantly beyond the contemporary paradigm of privacy in the United States. As discussed in Part III, transformations in technology and the increasing amount of personal information on individuals in the private sector have created an environment in which one need not have direct access to a secure government database in order to know sensitive information on a particular person. The gravity of this circumstance is compounded by the fact that the United States' adversaries have taken stock in U.S. dependence on information technology, harvesting and leveraging personal data with almost complete impunity.

As the amount of data on individual persons and entities increases, there will be ever-increasing opportunities and incentives to leverage such data to accomplish any number of tactical, operational, or strategic objectives in diplomacy, war, or simply criminal enterprise. The U.S. concept of privacy as an administrative check on the government's intrusion into the lives of its citizens no longer aligns with an operational environment in which the most heightened risks to privacy, particularly the privacy of government employees and service members, come from hostile, non-governmental actors. Likewise, the theory that individuals can be empowered negotiators in the collection, use, and sharing of their personal information by private industry no longer holds weight.

Without question, U.S. society's paradigm for privacy has reached critical mass. If this crisis originated in government information practices, it would seem reasonable to focus on government agencies' compliance with the Privacy Act. Yet, the crisis did not emerge, at least exclusively, from the government's

230. E-Government Act of 2002, Pub. L. No. 107–347, 116 Stat. 2946 (Federal Information Security Management Act).

handling of personal information. A heightened mistrust of government is appropriate from the perspective of protecting an individual's civil liberties in the face of ever-evolving government surveillance technologies; however, such mistrust undermines the protective role that the U.S. government can play in the face of an unregulated, hostile information environment.

The U.S. paradigm for privacy must shift, from a paradigm dominated by citizens' mistrust of government to one that is more nuanced and accommodating of government stewardship. The following recommendations address ways to facilitate this shift and how to re-conceptualize privacy as an operational dimension of U.S. national security.

A. Privacy as an Operational Dimension of U.S. National Security

Americans should not settle for a fragmented, ad hoc approach to privacy. Although contemporary arguments in favor of a federal omnibus law on privacy are a step in the right direction,[231] the continuous level of engagement that would be required to keep up with the pace of technology's impact on privacy warrants a more enduring, unified commitment from the U.S. government.

1. Congressional Committees on Cybersecurity and Personal Information

Today, cybersecurity stands out as one of the greatest challenges to the security of governments, individuals, and businesses worldwide,[232] yet, in spite of this circumstance, "[n]o. . . congressional committee maintains primary responsibility for the numerous issues related to cybersecurity."[233] As one lawmaker stated, "some 80 groups claim some jurisdiction over cybersecurity," which can effectively slow down, if not impede, cyber legislation.[234] The diffuse nature of cybersecurity lawmaking is compounded by the ever-increasing complexity of the cybersecurity field.[235]

To increase the efficiency and profile of cybersecurity and privacy lawmaking and oversight, Congress should consider a re-organization of its committee

231. *See generally* Cameron Kerry, *Will This New Congress Be the One to Pass Data Privacy Legislation?*, LAWFARE BLOG (Jan. 11, 2019), https://www.lawfareblog.com/will-new-congress-be-one-pass-data-privacy-legislation.

232. Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who and How It Works*, 5 J.L. & CYBER WARFARE 147, 150 (2016).

233. *Id.* at 153 (2016); *cf.* Cybersecurity and Infrastructure Security Agency Act of 2018, 6 U.S.C. § 652 (2019) (establishing the Cybersecurity and Infrastructure Security Agency (CISA)).

234. *See* Jack Corrigan, *Lawmaker: Congress Needs Fewer Committees with Cyber Oversight*, NEXTGOV (Jan. 29, 2019), https://www.nextgov.com/cybersecurity/2019/01/lawmaker-congress-needs-fewer-committees-cyber-oversight/154506/ (citing commentary from Rep. Jim Langevin).

235. Kate Patrick, *Congress Still Doesn't Understand Cybersecurity*, INSIDE SOURCES (Dec. 18, 2018), https://www.insidesources.com/congress-still-doesnt-understand-cybersecurity/ ("[P]art of the problem is that neither the private or the public sectors foster a robust cybersecurity culture."); *see also* Jory Heckman, *GAO Growing Cyber Staff Even If Congress Doesn't Revive Tech Assessment Office*, FEDERAL NEWS NETWORK (Feb. 28, 2019), https://federalnewsnetwork.com/hiring-retention/2019/02/gao-growing-cyber-staff-even-if-congress-doesnt-revive-tech-assessment-office/ (discussing the debate on how to reinvigorate technological expertise in the legislative branch via increased cybersecurity expertise in GAO or possibly re-establishment of the now defunct Office of Technology Assessment).

structure and their relevant assignments with an eye toward identifying only one or a few select committees responsible for cybersecurity and privacy matters. Paring down the number of committees involved in these highly technical fields presents a two-edged sword. As a disadvantage, the workload for these committees would likely significantly increase. However, by focusing efforts on a narrower subset of topics and issues, the re-organized committee(s) would be better prepared to tackle the most complex matters facing the United States in the information environment.

The alternative to this approach would be continuing with the status quo, in which jurisdiction over matters of cybersecurity and privacy is spread out over numerous committees.[236] A positive consequence of spreading out such large topic areas over numerous committees is the ability to manage divergent risks and tackle problems from different angles and through different entry points. In effect, legislative action can still be achieved through one or more committees despite inertia that may prevail in others.[237] The status quo, however, also lends itself to the ad hoc, fragmented approach that contributes to the crisis in privacy (and cybersecurity) today.

2. Privacy and Cyber Czars[238]

As discussed in Part III, the ad hoc, fragmented approach to privacy contributes to a disjointed patchwork of different privacy policy regimes and jurisdictions. OMB is responsible for setting privacy policy and ensuring compliance within the U.S. executive branch, and it executes this function through a number of key officials within each agency, such as the senior agency officials for privacy and privacy program managers. In addition, the Federal Privacy Council is responsible for advising and coordinating on the improvement of government privacy practices for their respective agencies and entities,[239] and the Privacy and Civil Liberties Oversight Board operates as an independent, bipartisan agency that is responsible for reviewing actions of the executive branch to ensure they comport with privacy and civil liberties protections.[240] Although all of these entities, in principle, work together in addressing issues of privacy, their focus is on matters within the federal government, and in particular the executive branch.

---

236. Trautman, *supra* note 232, at 180 (describing all of the various committees involved in cybersecurity as of 2015).

237. *See, e.g.*, Tim Starks & Eric Geller, *Where Cybersecurity Legislation 'Goes to Die' in Congress*, POLITICO (Feb. 11, 2019), https://www.politico.com/story/2019/02/11/cybersecurity-ron-johnson-1160081?utm_source=Sailthru&utm_medium=email&utm_campaign=EBB%2012.02.19&utm_term=Editorial%20-%20Early%20Bird%20Brief (discussing different perspectives on the perceived inertia as it pertains to cybersecurity-related bills presented to the Senate Homeland Security and Governmental Affairs Committee).

238. The informal term "czar" is used in media to refer to senior executive branch officials who oversee a particular policy. No U.S. government office has ever used the title "czar" to refer to their actual, official position.

239. Exec. Order No. 13,719, 81 Fed. Reg. 7961 (Feb. 9, 2016).

240. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, 118 Stat. 3638 (codified as amended at 50 U.S.C. § 401).

In the private sector, industry self-regulation dominates, and privacy policy is ad hoc, fragmented, and sector-based. Whereas, to a limited extent, the Cybersecurity and Infrastructure Security Agency (CISA) oversees the U.S. government's assistance to cybersecurity risks and incidents in the public and private sectors,[241] there is no single agency responsible for privacy matters in the private sector.[242]

The mission of the privacy czar would be to bring these communities together, not only for purposes of developing coherent U.S. government positions on privacy, but also identifying, assessing, and communicating risks to personal information of U.S. persons to the President and Congress.[243] The privacy czar would be a senior advisor to the President on privacy but would also be reportable to Congress.[244] A privacy czar could alleviate "international misunderstandings" on U.S. government privacy policy and serve as the point person for synthesizing or rationalizing the different sectoral interests and approaches to privacy.[245]

The concept of a privacy czar has been considered on a number of occasions before,[246] and there are notable criticisms. A privacy czar with limited powers to regulate agencies or the private sector may not have the necessary weight to effectively protect persons from actual abuses.[247] Alternatively, a privacy czar with some power may take strong pro-privacy positions that could impact the free flow of information, which has been a common complaint of European Union approaches to privacy.[248] Although these criticisms warrant consideration in the details of creating the position, they do not undermine the fact that a senior-level official on privacy is needed to cut across the disparate privacy regimes that have contributed to the current crisis in the protection of personal information. The same argument holds true for the now defunct cyber czar position.

Privacy and cyber czars would complement each other in the same way that the chief information officer (CIO) and senior agency official for privacy work together in identifying and resolving risks to security and privacy. Under former President Obama, the cyber czar's role was to harmonize government policy on cybersecurity and digital warfare.[249] The re-creation of the cyber and privacy czar positions would align with the current approach of dividing privacy and security

241. *See, e.g.*, Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115–278, 132 Stat. 4168.

242. Long & Quek, *supra* note 98, at 332; Shaffer, *supra* note 94, at 23.

243. *See* Alan Charles Raul, *After NSA Revelations, A Privacy Czar is Needed*, WASH. POST (Sept. 22, 2013), https://www.washingtonpost.com/opinions/after-nsa-revelations-a-privacy-czar-is-needed/2013/09/22/d2ada81c-219b-11e3-966c-9c4293c47ebe_story.html?utm_term=.51b21e9ff48c.

244. *Id.*

245. *Id.*

246. During President Clinton's administration, Peter Swire served as chief privacy counselor to the President.

247. Jonathan M. Winer, *Regulating the Free Flow of Information: A Privacy Czar as the Ultimate Big Brother*, 19 J. MARSHALL J. COMPUTER & INFO. L. 37, 38 (2000).

248. *Id.*

249. Eric Walsh, *Trump Scraps Cyber Czar Post After First Appointee Leaves: White House*, REUTERS (May 15, 2018), https://www.reuters.com/article/us-usa-cyber-whitehouse/trump-scraps-cyber-czar-post-after-first-appointee-leaves-white-house-idUSKCN1IG3GG.

concerns within executive-level agencies. Working together, a privacy and cyber czar could serve as "architects" and "spokespersons" for re-conceptualizing privacy as an operational dimension of U.S. national security.

3. International Law on the Use of Personal Information as an Attack Vector

Cyber operations are still a relatively new field in international law.[250] Treaty law governing the cyberspace is sparse, and customary international law specific to the information environment is exceptionally limited.[251] Efforts to define customary international cyber law by applying existing international treaties and norms to the information environment provide persuasive authority on the *lex lata* for the information environment;[252] however, persuasive perspectives do not necessarily constrain, regulate, or prevent attacks.[253] If attacks on personal information can achieve destruction on par with attacks on physical objects and structures,[254] then new norms, and ultimately legal conventions, must be created to prevent or at least mitigate the likely future scenarios of devastating digital catastrophes.

As the digital world becomes increasingly integrated with the basic functions and routines of physical life,[255] we have to recognize that an attack on a digital persona can qualify as an attack on one's physical well-being.[256] At this stage in the emerging information world, the relationship between an attack on one's digital persona and a deadly attack on one's physical person may seem too tenuous.[257] However, "the strategic significance of hyperconnectivity cannot be overstated."[258] The only barrier to the worst possible manifestations of the rapidly evolving information environment is the imagination.[259] Understanding the digital self to be an appendage of one's physical health and well-being will translate

250. *See* TALLINN MANUAL, *supra* note 205, at 3.

251. *Id.*

252. *Id.*

253. *See generally* Tarah Wheeler, *In Cyberwar, There Are No Rules: Why the World Desperately Needs Digital Geneva Conventions*, FOREIGN POLICY (Sept. 12, 2018), https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/.

254. *See, e.g.*, *id.* (comparing the attack on Sony Pictures to the physical destruction of a Texas oil field or an Appalachian coal mine. "If such a valuable civilian resource had been intentionally destroyed by a foreign adversary, it would be considered an act of war.").

255. *See, e.g.*, BOUSKILL, CHONDE & WELSER, *supra* note 14, at 8 (describing different futuristic scenarios in which speed will accelerate human life, one of which includes "removable cognitive implants (RCIs) that enable rapid training of human physical and cognitive capabilities and instantaneous messaging between users[.]").

256. Wheeler, *supra* note 253 (describing various examples of attacks on data, one of which could include sending a text message to civilian pilots of an emergency or other event that could prompt chaos in the U.S. air transportation system, which could lead to dangerous consequences).

257. TALLINN MANUAL, *supra* note 205, at 437 (describing the view of the majority of the International Group of Experts that the law of armed conflict notion of military or civilian object is "not to be interpreted as including data, at least in the current state of the law. In the view of these Experts, . . . an attack on data *per se* does not qualify as an attack.").

258. NATHAN P. FREIER ET AL., STRATEGIC STUDIES INSTITUTE, AT OUR OWN PERIL: DOD RISK ASSESSMENT IN A POST-PRIMACY WORLD 54 (2017).

259. *Id.*

into norms and protocols for the management of personal information. Re-conceptualizing personal information as an essential and indistinguishable attribute of citizens may also lead to a determination that personal information, in certain contexts, must be deemed a critical national security asset.[260]

B. Privacy Program Operationalization

In the wake of the 9/11 terrorist attacks, the U.S. Congress and the President created the 9/11 Commission to investigate the facts and circumstances relating to the attacks.[261] The commission identified failures in the U.S. government that preceded the attacks – specifically, failures in imagination, policy, capabilities, and management.[262] The description of these failings provides a useful overlay for, and a sober introduction to, the operationalization of privacy.

Imagination is not an attribute of bureaucracies.[263] In the years preceding 9/11, there were reports and analyses of al Qaeda, but there was no "complete portrait" of the organization's strategy and no "collective debate by the U.S. government" on the nature of the threat.[264] Similarly, although there have been congressional hearings, committee reports, and academic or operational ponderings related to the hacking of databases and exploitation of personal information, the destructive power of this phenomenon as a type of warfare has yet to capture the collective imagination of policy makers, commanders, and individual Americans.[265]

As the commission also pointed out in its report, the road to 9/11 was littered with opportunities for the formulation of national policy;[266] however, in light of a threat that was not entirely understood, let alone appreciated, the costs and risks associated with various courses of action seemed too high to prompt collective action.[267] Of course, if someone is a victim of identity theft, the impact is tangible and deserving of a response to that person; however, few Americans appear to see their personal information exposed to such a degree as to cause them to

260. *See generally* JOHN MOTEFF & PAUL PARFOMAK, CONG. RESEARCH SERV., RL32631, CRITICAL INFRASTRUCTURE AND KEY ASSETS: DEFINITION AND IDENTIFICATION 14 (2004) (discussing the ever-evolving definition of critical infrastructure and assets). Though not mentioned, one questions whether (or rather when) personal information may assume a level of significance that under certain circumstances it could qualify as a critical asset to the sustainability of critical infrastructure or critical segments of society.

261. Intelligence Authorization Act for Fiscal Year 2003, Pub. L. No. 107–306 § 601, 116 Stat. 2383, 2408.

262. *See* THOMAS H. KEAN ET AL., NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 339–360 (2004).

263. *See* Daniel A. Farber, *"Beyond Imagination" : Government Blind Spots Regarding Catastrophic Risks*, 11 ISSUES LEGAL SCHOLARSHIP 5, 5 (2013), https://ssrn.com/abstract=2295767.

264. KEAN ET AL., *supra* note 262, at 342–43.

265. *See Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELATIONS (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection/ (describing lawmakers' failure to address privacy, making the United States a "global outlier" in data protection).

266. *See* KEAN ET AL., *supra* note 262, at 348-350.

267. *Id*. at 350-52.

change their routines.[268] The 9/11 commission's statement rings prescient: "It is hardest to mount a major effort while a problem still seems minor. . .[however], once the danger has fully materialized, evident to all, mobilizing action is easier – but it then may be too late."[269] The 9/11 commission speculated that Bin Laden may have inferred that attacks on the United States, on a limited level like the attack on the U.S.S. Cole, would be possibly "risk free."[270] One wonders if the same consideration may be true for those hostile actors currently harvesting personal information today.

"The details of what happened on the morning of September 11 are complex, but they play out a simple theme. NORAD and the FAA were unprepared for the type of attacks launched against the United States on September 11, 2001."[271] Lacking the training for such a scenario, the officers and personnel who responded to the events of September 11 had to improvise.[272] Despite the vast bureaucracy dedicated to ensuring the security of government information systems and the smaller (but no less significant) cadre of government officials dedicated to the privacy and civil liberties of U.S. persons, the U.S. government has not prepared for a scenario in which the United States is the victim of a strategically-significant attack on its institutions through the weaponization of personal information outside the physical or digital confines of the government.[273]

Interagency priority setting, planning, and coordination was also a critical failure in the lead-up to the 9/11 attacks. Information within the U.S. government was not shared or, if it was provided, it was not timely or given in a context that prompted action or elevated concern.[274] In the current privacy scheme, there are clear processes, systems, and structures in place to manage the government's collection, sharing, use, and retention of personal information.[275] There are also processes, systems, and structures in place to manage the cybersecurity of the homeland.[276] However, the bureaucracy has not adapted to an information environment in which a hostile actor may not even need to access a government information system or use critical infrastructure data in order to wreak considerable damage on U.S. persons, institutions, and interests.[277] Seemingly innocuous, personal information can be leveraged to generate friction, confusion, and chaos

268. Jessica Dickler, *41 Million Americans Have Had Their Identities Stolen*, CNBC (Oct. 11, 2016), https://www.cnbc.com/2016/10/10/41-million-americans-have-had-their-identities-stolen.html.

269. KEAN ET AL., *supra* note 262, at 350.

270. *Id.*

271. *Id.* at 45.

272. *Id.* at 315.

273. *See generally* William R. Gery, SeYoung Lee & Jacob Ninas, *Information Warfare in an Information Age*, 85 JOINT FORCE Q. 22 (2017), https://ndupress.ndu.edu/Media/News/Article/1130649/information-warfare-in-an-information-age/.

274. *See, e.g.*, KEAN ET AL., *supra* note 262, at 353-57 (discussing information exchanged between the FBI, CIA, and FAA about the hijackers).

275. *See generally* Part I.

276. *See, e.g.*, Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115–278, 132 Stat. 4186.

277. *See* Wheeler, *supra* note 253.

across the information battlespace in order to diminish, alter, or defeat the exercise or projection of U.S. power.

Drawing from these considerations, the following recommendations aim to provide concrete ways in which to re-conceptualize privacy in operational terms.

1. Expand Privacy Program Officer Authorities and Responsibilities

Because privacy program officers operate as organizational experts on privacy and the protection of personal information, they stand out as the most optimum advisers for informing organizations and personnel on risks to personal information both inside and outside the organization while preserving the privacy and civil liberties of relevant persons. Privacy program officers should be given the authority, role, and responsibility of helping government and relevant personnel in the security of their personal information. They should also be responsible for advising the organization on risk to mission, based on macro-level "sight pictures"[278] of employee and service members' personal information exposure in the information environment. To state this another way, the privacy officer is looking at the various points across the information landscape in which personal information of relevant personnel is exposed to attack from an adversary and reporting on these vulnerabilities to organizational leadership. These sight pictures, snapshots, or assessments can speak to any range of information nodes, services, or behaviors in which personal information may be exposed to attack. For example, an attack on a social media service provider would generate an obligation on the part of the privacy officer, in collaboration with relevant security experts, to report not only this attack but also its potential second- and third-order effects on an organization should such an attack be leveraged to directly or indirectly target an organization's ability to accomplish a function or mission.

As a matter of routine, U.S. security organizations review the public profiles of other U.S. government personnel, job applicants, and cleared personnel. Formalizing and expanding the number of personnel who are subject to this process would not violate the privacy rights of government employees or service members. The exclusive aim of this process would be to assist the organization in its assessment of risk and facilitate better awareness of, and ultimately response plans for, the threat environment as it relates to their employees, service members, and dependents.

Of course, many government employees and members of the military may balk at such a requirement. Personnel and their dependents may perceive any interest in their public profile as subterfuge for government surveillance. To facilitate trust and ensure the protection of privacy and civil liberties, organizations must provide clear rules on how information will be collected, used, and shared. The initial phase of the work must be voluntary, and, in many organizational functions or areas, participation should remain voluntary. However, even if participation is voluntary, organizational privacy programs should require employees and service members to

278. A "sight picture" is essentially a term used to describe what one sees when he or she is looking at a particular point on the horizon through the aperture of an instrument or weapon.

receive training on the information domain and how to identify, respond, and report attacks on their personal information through organizational channels.

2. Develop New Strategic and Operational Doctrine

The U.S. government already sponsors various centers of excellence relating to cyber defense,[279] cyber operations,[280] and cybersecurity.[281] Although these centers address privacy to some extent, their focus is understandably specific to cyber operations. There have also been some limited efforts to establish small centers of excellence within the U.S. government related to specific privacy topics.[282] Notwithstanding these contemporary programs or efforts, for the most part, there is no center of excellence on privacy in the U.S. government.[283]

A center of excellence on privacy would assist in the development of new doctrine, training programs, and products related to the operationalization of privacy. In the same way that the privacy czar would bring together different communities and interests for developing coherent privacy policy at the national and international levels of U.S. government policy, a privacy center of excellence would focus on the strategic and operational levels of privacy to bring actionable input to established interagency and public-private processes, frameworks, standards, and norms. Apart from developing new doctrine and training, a center of excellence on privacy could also serve as the hub for working with private industry in addressing new trends, vulnerabilities, and technologies to ensure the continuous exchange of information on changes to the information environment.

Using information as a weapon of war is not a novel concept;[284] however, only recently have the DoD and the Services begun building and incorporating information warfighting doctrine into the operational and lower levels.[285] Drawing from doctrine, training programs, and products from a privacy center of excellence or other relevant institutions, leaders should build personal information security standdowns into their operational preparations and unit or agency security routines.

279. NAT'L SECURITY AGENCY, NATIONAL CENTERS OF ACADEMIC EXCELLENCE, https://www.nsa.gov/resources/students-educators/centers-academic-excellence/#defense (Mar. 15, 2019).

280. *Id.*

281. *Id.*

282. *See, e.g.*, *Center of Excellence for Protected Health Information Related to Mental and Substance Use Disorders: Initial Announcement*, SUBSTANCE ABUSE AND MENTAL HEALTH SERVS. ADMIN. (May 17, 2019), https://www.samhsa.gov/grants/grant-announcements/ti-18-021.

283. *See generally* Gery, Lee & Ninas, *supra* note 273.

284. *See generally* DOD STRATEGY FOR OPERATING IN THE INFORMATION ENVIRONMENT, *supra* note 117.

285. *See, e.g.*, DEP'T OF THE NAVY, MARINE CORPS BULL. NO. 5400: ESTABLISHMENT OF INFO. AS THE SEVENTH MARINE CORPS WARFIGHTING FUNCTION (2019); *see generally* Terron Wharton, *Viral Conflict: Proposing the Information Warfighting Function*, SMALL WARS J. (2017), https://smallwarsjournal.com/jrnl/art/viral-conflict-proposing-the-information-warfighting-function. (discussing the shortfall in the Army's warfighting doctrine as it relates to information warfighting function); Nick Brunetti-Lihach, *Information Warfare Past, Present, and Future*, REAL CLEAR DEF. (Nov. 14, 2018), https://www.realcleardefense.com/articles/2018/11/14/information_warfare_past_present_and_future_113955.html; Mark Pomerleau, *Navy Creates Information Warfighting Development Center*, C4ISRNET (Feb. 24, 2017), https://www.c4isrnet.com/show-reporter/afcea-west/2017/02/24/navy-creates-information-warfighting-development-center/.

These stand-downs would be pre-planned, controlled pauses to normal operations to ensure personnel are educated and trained on the threat environment and how to identify, and what to do, if their personal information has been exploited. Leaders can give their personnel time to accomplish routine digital hygiene such as changing passwords and deleting information that exposes them to unnecessary risks, and they can work with information security teams to walk through hypothetical scenarios in which personal information can be leveraged to undermine, diminish, or defeat a particular agency function or mission. Exercises could include hypothetical attacks on select persons, units, or functions through their personal devices, profiles, or other means. Leaders should ask how their personnel and their organizations would identify and respond to attacks in the ramp-up to war or in the midst of a significant operation or activity. Leaders may also ask to what extent their respective unit or organization is practicing good information hygiene.

3. Develop and Implement Training Programs

Human error is very often the weakest link in cybersecurity. "While we focus the vast majority of our security efforts on protecting computers and networks, more than 80% of cyber attacks and over 70% of those from nation-states are initiated by exploiting humans rather than computer or network security flaws."[286] The Russian attack on the DNC during the 2016 presidential elections illustrates this point.

Although there were a number of failures and vulnerabilities that contributed to the DNC's exposure to attack, one of the most prominent circumstances was human error. During the presidential campaign, John Podesta, campaign manager for Hillary Clinton, received the following message, which encouraged him to click on the link "CHANGE PASSWORD":

> Subject: Someone has your password
>
> Hi John
> Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.
>
> Details: Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
> Google stopped this sign-in attempt. You should change your password immediately.
>
> *CHANGE PASSWORD*
>
> Best,
> The Gmail Team

286. Wade Shen, *Active Social Engineering Defense (ASED)*, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, https://www.darpa.mil/attachments/ShenASED.pdf.

Mr. Podesta's chief of staff, Sara Latham, forwarded the email to Charles Delavan, who was the information technology professional employed by the DNC at that time. Mr. Delavan responded with the following message.

> Sara,
>
> This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.
>
> He can go to this link: https://myaccount.google.com/security to do both. It is absolutely imperative that this is done ASAP.
>
> If you or he has any questions, please reach out to me at [redacted]

The aforementioned exchange has become an infamous case study in hacking. It is still unclear whether Mr. Delavan fell for the ruse or, as a consequence of a misinterpretation of his email, Mr. Podesta or other staff members clicked on the link. What is clear is that clicking on the link gave Russian hackers "a decade's worth of Mr. Podesta's emails (60,000 in total)."[287]

According to a survey done in 2017, more than 9 in 10 Americans (94%) have heard news of security breaches in the past year, but over 2 out of 5 (43%) have not altered their online habits as a result of this news.[288] In addition, only 26 percent of Americans have used a credit monitoring service in the past 12 months.[289] Despite the widespread targeting of personal information and the increasing ability of malevolent actors to leverage such information for exploitative gain, the U.S. government, and particularly DoD, should take heed that many employees and service members may not have a basic understanding of the threat environment or what to do if their personal information is exposed or targeted.

Under current policies, a service member or employee can receive any number of ad hoc, and sometimes generic, emails, notices, or other communications from cybersecurity professionals warning them of significant attempts to target their emails or other personal information in the information domain. Unfortunately, there is no standard training package, let alone organizational or enterprise training policies for employees, service members, contractors, or dependents.[290] A

287. *A Single Typo May Have Tipped U.S. Election Trump's Way*, IT SECURITY GURU (Dec. 14, 2016), https://www.itsecurityguru.org/2016/12/14/single-typo-may-tipped-us-election-trumps-way/; *see* Eric Lipton, *How We Identified the D.N.C. Hack's 'Patient Zero'*, N.Y. TIMES, (Dec. 20, 2016), https://www.nytimes.com/2016/12/20/insider/how-we-identified-the-dnc-hacks-patient-zero.html.

288. Jennifer Johnson, *New Study: Many Consumers Lack Understanding of Basic Cyber Hygiene*, TENABLE (Dec. 18, 2017), https://www.tenable.com/blog/new-study-many-consumers-lack-understanding-of-basic-cyber-hygiene.

289. *Id.*

290. DoD imposes annual "cyber awareness" training requirements that touch upon the issues raised in this paper; however, the training is basic and focused almost exclusively on attacks on, or compromises to, an individual's government computer, email accounts, or other mobile devices. *See* Stars and Stripes, *'Tina, You're a Fraud!': YouTube Star PewDiePie Takes the Cyber Awareness*

training plan should require input from not just privacy, cybersecurity, and intelligence and counterintelligence fields, but also private industry.

4. Develop Expanded Risk Assessment and Response Plans

Organizations need to consider the risk of attack on personal information on employees, dependents, and support staff *outside* the organization as part of their organizational risk assessment. Input from this study would assist the organization in developing decision-making tools on how it would respond to contingencies in which the personal information of government and military personnel, third party associates, and dependents were attacked from outside of the organization's systems. Breach response teams would be better prepared with courses of action for senior leaders in the event of a coordinated attack on the personal information of government and military personnel, associates, and their dependents. In the absence of organization-based resources for response, then at least reporting could be forwarded up to higher echelons within the government for risk assessment, response, and mitigation.

Allowing organizations to look beyond the confines of their systems aligns, at least in conceptual terms, with the contemporary shift from perimeter-centric approaches to more defense-in-depth cybersecurity strategies.

> With the growing use of cloud, mobility and related technologies, as well as the focus on arming the warfighter on the frontlines with information, the network perimeter has all but disappeared, with threats coming in through countless attack vectors, including cloud applications, mobile devices/apps, and email. In this environment, defense agencies need to trust less in host-based, perimeter-centric security and focus more on data- and related application-level protections that extend wherever data might be, even remote, forward locations. Data is the new perimeter.[291]

Using data as the "new perimeter," certain members of the military and the government should be required to inform privacy officers on the types of accounts they maintain, web profiles, and other digital or information footprints for the purpose of giving such officers an ability to advise personnel on risks to their personal information and inform organizational risk assessments and response plans. The concept of requiring this information is not novel, nor is it *per se* intrusive.

Government personnel have to report foreign travel, close and continuous relationships with foreign citizens, and any number of personal life circumstances that could expose the individual to potential exploitation or recruitment by

---

Challenge, YOUTUBE (Aug. 10, 2018), https://www.stripes.com/news/tina-you-re-a-fraud-youtube-star-pewdiepie-takes-the-cyber-awareness-challenge-1.541913; *see also* PewDiePie, *Sponsored by USA – This Game Was Made by the Government…*, YOUTUBE (Aug. 9, 2018), https://www.youtube.com/watch?v=BlCXgpozrZg.

291. Aubrey Merchant-Dest, *supra* note 222.

foreign intelligence services.[292] The fact that the U.S. government places heightened scrutiny on the traditional levers and approaches of intelligence collection, without equal attention to the tools and exploits of the information landscape, suggests we are still fighting the wars of today and the future with yesterday's tradecraft.[293]

5. Develop and Implement Risk Mitigation Measures

There are relatively few options for relief for victims who find their personal information attacked. Through the Privacy Act, victims of unwarranted disclosures of their personal information held by the federal government can sue the federal government for damages;[294] however, the courts construe this civil remedy narrowly, allowing plaintiffs to only collect for "actual damages" caused by "intentional or willful" disclosures by a government official.[295] Since the hostile actor's intrusion or exploitation of personal information would be the dominant reason for the unwarranted violation of privacy, rather than an intentional or willful act by the government, it would seem difficult for victim-plaintiffs to obtain relief through the Privacy Act.[296] As limited as this channel of relief may be, it also would not address attacks on personal information in the private sector, which in comparison offers an exponentially greater attack surface.[297]

Victims can sue attackers under a variety of tort theories ranging from conversion, trespass to chattels, and civil remedy provisions under the federal Computer Fraud and Abuse Act; however, the possibility of restitution is very remote in those instances in which persons are located in other countries, which is frequently the case.[298] In an effort to stymie the increasing number and audacity of cyberattacks, the U.S. government has adopted a policy of "naming and shaming" individual hackers through public announcements of their criminal charges.

---

292. OFFICE OF MGMT. & BUDGET, OMB NO. 3206-0005, STANDARD FORM 86: QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS (2016).

293. *See, e.g.*, Warren Strobel & Jonathan Landav, *Exclusive: U.S. Accuses China of 'Super Aggressive' Spy Campaign on LinkedIn*, REUTERS (Aug. 31, 2018), https://www.reuters.com/article/us-linkedin-china-espionage-exclusive/exclusive-chief-u-s-spy-catcher-says-china-using-linkedin-to-recruit-americans-idUSKCN1LG15Y (describing, as a good case in point, the use of employment service platforms to target U.S. government personnel).

294. The Privacy Act of 1974, 5 U.S.C. § 552a(g) (1974).

295. *See* Doe v. Chao, 540 U.S. 614 (2004) (interpreting 5 U.S.C. § 552a(g)(4)).

296. *Cf.* Am. Fed'n of Gov't Emps. v. Hawley, 543 F. Supp. 2d 44 (D.D.C. 2008) (discussing the court's preliminary ruling that the claim was sufficient to survive summary judgment, in that the plaintiffs had shown that the government's negligence in establishing safeguards to protect personal information could be a contributing factor to the loss of such information when a government laptop was stolen. The preliminary ruling prompted the Transportation Security Agency (TSA) to settle the plaintiffs' claim, which meant the court did not reach the merits of the Privacy Act claim.).

297. *See* Bernard Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, FORBES (Mar. 21, 2018), https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#600358b760ba.

298. *See generally* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 259 (2005).

Whereas this policy may arguably achieve some long-term, strategic changes to nation-state behavior, it nevertheless achieves little in resolving the damage or punishing individuals involved in specific cases because the accused hackers "are rarely extradited to the United States."[299]

Database processors and entities holding the data that was breached could be held responsible for failing to prevent, mitigate, or respond to the breach; however, it seems difficult to impose liability on these agents if the attacks were either perpetrated or supported by a nation-state or alternatively when there is a state of war.[300]

Overall, there is no well-developed plan for helping persons who have been attacked through their personal information. Unlike other aspects of a person's well-being or financial security, personal information is not a customarily insured asset.

Personal information must be considered an insurable asset, the cost for which should be predominantly born by the individual employee or service member with some assistance from the U.S. government. If an employee or service member becomes ill or disabled, he or she would look to medical insurance with rates negotiated by the federal government. In an age in which one's personal information can be exploited and targeted for financial or other forms of ruin, there are many reasons to see the risk as one that should be integrated within one's portfolio of insurance services, and because these risks can translate into organizational risk, the U.S. government should consider it a prudent option to consider in overseeing employee and service members' well-being.

CONCLUSION

We stand at the precipice of the next great war – the opening to which will not likely occur on a sandy beach, grassy knoll, or dense urban landscape. Our near-peer competitors understand that strategic objectives do not have to be pursued according to the norms and protocols of the last century. The ubiquity of information and information technology has given rise to a new information domain that, when combined with asymmetric warfare strategies, allows for crucial victories to be secured without a single shot being fired. Despite the erosion of American power and the overwhelming signs of vulnerability to personal information, American society has not prepared for a scenario in which the weaponization of personal information becomes the pre-emptive strike or force multiplier for a high-end conflict. U.S. privacy law must shift from its over-reliance on the individual as the guardian of his or her personal information to a balanced approach

299. *See, e.g.*, Kate Fazzini & Kevin Breuninger, *Justice Department Charges Chinese Nationals in 'Extensive' Global Hacking Campaign*, CNBC (Dec. 20, 2018), https://www.cnbc.com/2018/12/20/doj-china-national-security-law-enforcement-action.html (discussing the Justice Department's charges against two Chinese nationals for attempting to steal intellectual property and personal data of more than 100,000 members of the U.S. Navy).

300. *See* Johnson, *supra* note 298, at 255 (discussing database possessor liability for harm caused by data intruders).

that acknowledges government (and organizations) as information stewards. Re-conceptualizing privacy as an operational dimension of U.S. national security can be achieved through a dynamic, forward-looking, adaptive approach built on training, cost mitigation, and an expanded and updated view of the operational value of personal information.

***