PUBLIC HEALTH AS A MODEL FOR CYBERSECURITY INFORMATION SHARING

Elaine M. Sedenberg[†] *& Deirdre K. Mulligan*[††]

ABSTRACT

Policy proposals often feature information sharing as a means to improve cybersecurity, but lack specificity connecting these activities to specific goals intended to advance the state of cybersecurity. We use the Doctrine of Cybersecurity as a lens to examine existing information sharing efforts and evaluate the utility of information sharing proposals. Leaning on the analogous public good-oriented field of public health, we extract insights on how these information policies and practices evolved to promote goals while actively mediating among values. Based on our review of specific public health information sharing systems, we derive a set of four principles—expert and collaborative data governance, reporting minimization and decentralization, earliest feasible de-identification, and limitations on use—to guide the development of information sharing proposals within the cybersecurity context, and include an analysis of specific sharing mechanisms—data access modes and sharing platforms—that inform the implementation of these four principles. We conclude with a set of recommendations for consideration within the context of cybersecurity information sharing proposals.

DOI: http://dx.doi.org/10.15779/Z38PZ61

[†] Elaine Sedenberg is a Ph.D. student at the University of California, Berkeley, School of Information, where she is a National Science Foundation (NSF) Graduate Research Fellow and a Berkeley Graduate Fellow. Previously, Elaine was a Science Policy Fellow at the Science and Technology Policy Institute (STPI) in Washington D.C., which is a Federally Funded Research and Development Center that supports the White House Office of Science and Technology Policy (OSTP), as well as the NSF and other agencies.

[††] Deirdre K. Mulligan is an Associate Professor in the School of Information at UC Berkeley and a co-Director of the Berkeley Center for Law & Technology. Prior to joining the School of Information in 2008, she was a Clinical Professor of Law, founding Director of the Samuelson Law, Technology & Public Policy Clinic, and Director of Clinical Programs at the UC Berkeley School of Law (Boalt Hall). She is Chair of the Board of Directors of the Center for Democracy and Technology, and a Fellow at the Electronic Frontier Foundation. Prior to Berkeley, she served as staff counsel at the Center for Democracy & Technology in Washington, D.C.

TABLE OF CONTENTS

I. INTRODUCTION

Information sharing figures prominently in policy proposals to improve cybersecurity, yet the connection between information sharing—*a means*—and specific cybersecurity goals has not been clearly or convincingly argued. In response to cybersecurity incidents,[1] Congress[2] and the White House[3] have made various proposals to promote information sharing between private industry and the U.S. government. These proposed frameworks and passage of recent legislation[4] lack specificity about the data to be shared and governing practices to be employed.[5] They also fail to adequately address civil liberties issues or articulate the overarching goals and specific objectives information sharing will advance.[6]

The lack of clarity around goals operates at two levels. First, cybersecurity conversations lack a strong doctrinal foundation from which

[1] Jose A. DelReal, *Eyes Turn to the Next Congress as Sony Hack Exposes Cybersecurity Flaws*, WASH. POST (Dec. 18, 2014), http://www.washingtonpost.com/blogs/post-politics/wp/2014/12/18/eyes-turn-to-the-next-congress-as-sony-hack-exposes-cybersecurity-flaws; Information About OPM Cybersecurity Incidents, U.S. OFFICE OF PERS. MGMT. (July 17, 2015), https://www.opm.gov/cybersecurity; Brian Krebs, *Posts Tagged: Target Data Breach*, KREBS ON SECURITY, http://krebsonsecurity.com/tag/target-data-breach/ (last visited Oct. 17, 2015).

[2] Cybersecurity Information Sharing Act, S. 754, 114th Cong. (2015), https://www.congress.gov/114/bills/s754/BILLS-114s754pcs.pdf.

[3] Exec. Order No. 13,691, Promoting Private Sector Cybersecurity Information Sharing, 80 Fed. Reg. 9349 (Feb. 20, 2015), https://www.archives.gov/federal-register/executive-orders/2015.html; Exec. Order No. 13,636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11,739 (Feb. 19, 2013), https://www.archives.gov/federal-register/executive-orders/2013.html.

[4] Consolidated Appropriation Act, 2016, Pub. L. No. 114-113, div. N, tit. I, https://www.congress.gov/114/bills/hr2029/BILLS-114hr2029enr.pdf (the "Cybersecurity Act of 2015"); *see also Congress Passes the Cybersecurity Act of 2015*, NAT'L L. REV. (Dec. 20, 2015), http://www.natlawreview.com/article/congress-passes-cybersecurity-act-2015.

[5] *See* Jennifer Granick, *The Right Way to Share Information and Improve Cybersecurity*, JUST SEC. (Mar. 26, 2015, 10:53 AM), http://justsecurity.org/21498/share-information-improve-cybersecurity (arguing that none of the plans proposed by Congress or the White House "narrowly and specifically identifies the categories of information that Congress wants to allow to be shared").

[6] *Cyber-Surveillance Bill to Move Forward, Secretly*, CTR. FOR DEMOCRACY & TECH. (Mar. 4, 2015), https://cdt.org/insight/cyber-surveillance-bill-to-move-forward-secretly/ (arguing that the Cybersecurity Information Sharing Act has moved "backwards in terms of privacy and civil liberties protections"); Mark Jaycox, *EFF to Congress: Stop the Cybersurveillance Bills*, EFF DEEPLINKS BLOG (Apr. 22, 2015), https://www.eff.org/deeplinks/2015/04/eff-congress-stop-cybersurveillance-bills (arguing that the Cybersecurity Information Sharing Act's "vague definition," as well as broad legal immunities for the government and companies, could lead to increased government surveillance and the sharing of information beyond the scope of cybersecurity objectives).

to evaluate proposed interventions. To what end is information sharing directed? Sharing information in and of itself will not improve cybersecurity. Policy proposals are motivated by a belief that information—that is currently unavailable to relevant parties—is necessary for certain cybersecurity-promoting activities. Yet, it is unclear exactly what activities policy makers want information sharing to fuel. What are recipients of information expected, or required, to do with information they receive? Whatever their private interest suggests? Or is there a broader shared set of public goals that should guide how recipients use this information? Is the goal of information sharing to aid law enforcement in identifying and prosecuting bad actors? Or is the goal to fuel vulnerability patching? Or is the hope that shared information will aid administrators in identifying and containing attacks in real time? Some combination of the three, or something else entirely? Clarifying the overarching goals of national cybersecurity policy is a precursor to a meaningful discussion about the likely effectiveness and relative appropriateness of sharing information.

Second, at the tactical level, current information sharing proposals do not specify the connections between the kinds of information to be shared and particular cybersecurity-promoting activities. Again, information may support activities that improve individual entities' security posture, or enable some broader vision of cybersecurity, or both, but current proposals fail to make these connections or direct activity toward specific ends. In this environment, information sharing is debated in the abstract with little attention to its role in an overall strategic national agenda, and with insufficient details to consider how access to specific information can support tactical activities that advance national priorities.

The lack of clear cybersecurity goals and nuanced tactical examination impedes the tough conversations about how to weigh and protect other values in our efforts to improve cybersecurity—including privacy, freedom of expression, innovation, and competition. In those cases where information sharing makes for sound policy, this lack of clear goals and tactics precludes the careful construction of laws and mechanisms to mediate tensions between cybersecurity goals and other values.

Our objective is to advance the policy deliberations about information sharing as a means to advance cybersecurity. We do so in two ways. First, we situate the consideration of information sharing within the broader understanding that cybersecurity is a public good. Second, drawing from the analogous area of public health, we offer a set of principles to guide policy makers in the construction of information sharing arrangements that prioritize, mitigate, and manage tensions among public values, and between the public good and private interests.

Part II positions the conversation about information sharing within the context of a growing agreement that cybersecurity is both a national priority and a public good. We concur with those who argue that, due to a range of public goods failures, individual market choices under-produce cybersecurity and therefore the state must play a role in advancing cybersecurity. We use the Doctrine of Public Cybersecurity[7] to evaluate the utility of information sharing. Under that doctrine, the goals of cybersecurity policy are to produce more secure artifacts and systems, and to promote security protective behaviors and effective management of the ongoing vulnerabilities that emerge from a constantly changing threat landscape. Viewed through this lens, the question is how and under what conditions information sharing can advance these twin goals of improving the security of systems and managing residual insecurity. We briefly review existing information sharing activities in the cybersecurity area to examine their relationship to these goals.

Next, in Part III, we explore the rich and diverse information sharing policies and practices in the analogous field of public health, and consider the utility and limitations of these approaches in advancing public cybersecurity goals.

In Part IV, we review specific public health policies and practices around information sharing, paying particular attention to those that mitigate the impact of public health activities on other public values and private interests. First, we show how information sharing plays an essential role in specific prevention and response activities within public health, and is facilitated through diverse mechanisms that combine law, policy, and technical approaches to manage competing interests and values. Second, we derive a set of four principles from the public health information sharing ecosystem—expert and collaborative data governance, reporting minimization and decentralization, earliest feasible de-identification, and limitations on use—to guide the development and consideration of information sharing proposals in the cybersecurity context. We conclude Part IV with an analysis of specific sharing mechanisms—data access modes and sharing platforms—that have the potential to inform implementation of the four principles.

In Part V we use these four principles derived from public health to develop a set of recommendations to guide the consideration of

[7] *See infra* Part II.

cybersecurity information sharing proposals. We recommend combining public-use practices, open data sets, and more limited information sharing regimes—coupled with limits on non-cybersecurity related uses of shared data—to advance public cybersecurity goals.

II. INFORMATION SHARING THROUGH THE DOCTRINE OF PUBLIC CYBERSECURITY

Cybersecurity information sharing proposals should be evaluated based on their capacity to address public goods related failures that hamper the production of more secure systems, and limit the ability to identify and respond to ongoing security vulnerabilities. We adopt the Doctrine of Public Cybersecurity as our frame for considering the utility of information sharing generally, and briefly analyze existing cybersecurity information sharing activities through its lens.

A. CYBERSECURITY AS A PUBLIC GOOD

Cybersecurity is an important domestic and international priority. Successful attacks on critical infrastructure,[8] strategic national assets,[9] personal information,[10] and corporate secrets[11] all stem from vulnerabilities in the interconnected socio-technical systems commonly referred to as the Internet. Such systems store personal and corporate secrets, help us connect and manage critical infrastructure, and form the communication and coordination backbone for the country.

The current state of cybersecurity is viewed as insufficient to protect the national, corporate, and personal activities entrusted to the Internet.[12]

[8] *See* INDUS. CONTROL SYS. CYBER EMERGENCY RESPONSE TEAM (ICS-CERT), ICS-CERT MONITOR: SEPTEMBER 2014-FEBRUARY 2015, at 2 (2015), https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf.

[9] *See* Trevor Hughes, *Calif. Attacks Send Warning that Internet Lines are 'Basically Unsecured,'* USA TODAY, (July 1, 2015, 8:31 PM), http://www.usatoday.com/story/tech/2015/07/01/california-internet-service-restored/29563899/; ICS-CERT MONITOR, *supra* note 8.

[10] *See* Krebs, *supra* note 1.

[11] *Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats? Hearing Before the Subcomm. on Crime & Terrorism of the S. Comm. on the Judiciary*, 113th Cong. (2014) (statement of Randall C. Coleman, Assistant Director, Counterintelligence Division, FBI), https://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft.

[12] *See* JASON, JSR-10-102, SCIENCE OF CYBER-SECURITY 9 (2010), http://fas.org/irp/agency/dod/jason/cyber.pdf; MINORITY STAFF OF HOMELAND SEC. AND GOVERNMENTAL AFFAIRS COMM., THE FEDERAL GOVERNMENT'S TRACK RECORD ON CYBERSECURITY AND CRITICAL INFRASTRUCTURE 2 (2014),

The failure of the market to produce adequate investments in information security is well-documented,[13] and explained by its public good qualities. Researchers have identified several public good characteristics that contribute to the chronic underproduction of cybersecurity.[14] Due to the network effects of security investments, individual actors are unable to reap the full value of their cybersecurity investments, or to limit their risk through independent investments.[15] Information asymmetry, combined with the misaligned incentives that these externalities cause, contribute to poor cybersecurity investments and management.[16] Further depressing investment in cybersecurity is the difficulty in assessing both risk and return on investment, which in turn creates difficulties for security professionals who must argue for dollars without strong metrics for success.

http://www.hsgac.senate.gov/download/the-federal-governments-track-record-on-cybersecurity-and-critical-infrastructure (prepared by Sen. Tom Coburn); DEP'T OF HOMELAND SEC., ENABLING DISTRIBUTED SECURITY IN CYBERSPACE: BUILDING A HEALTHY AND RESILIENT CYBER ECOSYSTEM WITH AUTOMATED COLLECTIVE ACTION 5 (2011), http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

[13] Alessandro Acquisti, William Horne & Charles Palmer, *Cyber Economics*, *in* NATIONAL CYBER LEAP YEAR SUMMIT 2009 CO-CHAIRS' REPORT 25, 25 (2009), https://www.nitrd.gov/nitrdgroups/images/b/bd/National_Cyber_Leap_jYear_Summit_2009_CoChairs_Report.pdf; BRENT R. ROWE & MICHAEL P. GALLAGHER, PRIVATE SECTOR CYBER SECURITY INVESTMENT STRATEGIES: AN EMPIRICAL ANALYSIS 2 (2006), http://www.econinfosec.org/archive/weis2006/docs/18.pdf (presented at the Fifth Workshop on the Economics of Information Security); Amitai Etzioni, *Cybersecurity in the Private Sector*, 28 ISSUES SCI. & TECH. 58, 59 (2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2356955.

[14] The first malware, the Morris Worm in 1998, propagated at such a fast rate it infiltrated and compromised (often shutting down) computers across the Internet, including U.S. military sites. THOMAS K. CLANCY, COMPUTER CRIME AND DIGITAL EVIDENCE: MATERIALS AND CASES 500 (2011). There are many examples of botnets, that when left unpatched or uncontained, end up impacting government computers or contractors. *See, e.g.*, Brian Krebs, *U.S. Government Takes Down Coreflood Botnet*, KREBS ON SECURITY (Apr. 11, 2014), http://krebsonsecurity.com/2011/04/u-s-government-takes-down-coreflood-botnet.

[15] For example, Microsoft changed their security update policy to include pirated copies of Windows operating system because patching has a positive network effect on all Windows machines—legal or pirated alike. Ina Fried, *Piracy-Check Mandatory for Windows Add-Ons*, CNET (July 26, 2005), http://www.cnet.com/news/piracy-check-mandatory-for-windows-add-ons/; Lawrence M. Walsh, *Pirated Software Security: Patching Pirated Software*, TECHTARGET (Mar. 2004), http://searchsecurity.techtarget.com/Pirated-software-security-Patching-pirated-software; ROWE & GALLAGHER, *supra* note 13, at 2.

[16] Etzioni, *supra* note 13, at 59; Esther Gal-Or & Anindya Ghose, *The Economic Incentives for Sharing Security Information*, 16 INF. SYST. RES. 186, 187 (2005).

Despite recognition of these public good related challenges, cybersecurity policy has not been oriented to address them. Historically, cybersecurity policy has—for the most part implicitly—been shaped by the goals of deterrence reflected in criminal laws, and by risk management principles reflected in process-oriented security standards.[17]

Prior work urged the adoption of the Doctrine of Public Cybersecurity to orient public policy and private sector activities toward addressing these public good related challenges.[18] This work argues that cybersecurity policy should aim to spur the production of more secure systems, security-promoting behaviors, and activities to manage and respond to ongoing insecurity. The Doctrine of Public Cybersecurity steers policy makers away from less fruitful orientations, such as the deterrence-oriented strategies reflected in current criminal law, which do little to encourage the production of cybersecurity or to manage cyber-insecurity. We believe this is the correct orientation for national cybersecurity policy.

We use the Doctrine of Public Cybersecurity to explore the utility of information sharing. Through this lens, information sharing is valuable when it supports the production of more secure systems and behaviors, and/or aids in the management of and response to ongoing vulnerabilities. To the extent they are deemed useful to advance these two goals, information sharing policies and technical mechanisms should be considered, but only where constructed with affordances and constraints that attend to other competing public and private values.

B. INFORMATION SHARING AS A MEANS TO ADVANCE PUBLIC CYBERSECURITY GOALS

Today's cybersecurity environment boasts a wide range of information sharing activities. Some, like industry specific Information Sharing and Analysis Centers (ISACs)[19] and the United States Computer Emergency Readiness Team (US-CERT),[20] are long standing and supported by the government to promote sharing between trusted communities or industry-specific partners, as well as the public. Information Sharing and Analysis

[17] Deirdre K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity*, 140 DAEDALUS 70 (2011).

[18] *Id.*

[19] *About Us*, NAT'L COUNCIL OF INFORMATION SHARING & ANALYSIS CTRS. (ISACS), http://www.isaccouncil.org/aboutus.html (last visited Aug. 12, 2015).

[20] *About Us*, U.S. COMPUTER EMERGENCY READINESS TEAM (US-CERT), https://www.us-cert.gov/about-us (last visited Aug. 12, 2015).

Organizations (ISAOs)[21] were recently added to complement existing ISACs and offer an alternative organization outside of specified industries (e.g., region, sector, sub-sector, etc.). Other information sharing activities have arisen independently in response to specific threats either discrete or ongoing, and have largely been the product of private decisions by security practitioners and their employers. Some are aimed at improving specific products, while others focus on sharing best practices, or on identifying and managing attacks. We briefly examine some existing efforts to highlight their diversity and their relationships to public cybersecurity goals, and note some organizational shortcomings and opportunities for improvement.

1. *Information Sharing to Improve Artifacts, Policies, and Practices*

a) Sharing Information About Vulnerabilities

There is a rich information market (white hat and black hat) for the discovery and exchange of information about vulnerabilities and exploits.[22] Vulnerability rewards programs (VRPs), also known as "bug bounties," incentivize the reporting of information to organizations (namely software vendors) so that they can create patches to prevent exploitation. These programs are designed to promote disclosure to those in the position to patch them since discovered—but unreported—vulnerabilities may be sold on the black market as zero-day exploits (exploitable software vulnerabilities unknown to the vendor). However, the effectiveness and value of these programs is debated since vulnerabilities often command a higher price on the black market,[23] and some argue the commercialization of vulnerability information limits the availability of data and knowledge within security research.[24] Not all vendors utilize VRPs, but those that do offer varying participation guidelines and incentive structures, often

[21] Exec. Order No. 13,691, 80 Fed. Reg. 9349 (Feb. 13, 2015), https://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf.

[22] Serge Egelman, Cormac Herley & Paul C. van Oorschot, *Markets for Zero-Day Exploits : Ethics and Implications*, 2013 NEW SEC. PARADIGM WORKSHOP 41, 41 (2013); LILLIAN ABLON, MARTIN C. LIBICKI & ANGREA A. GOLAY, RAND CORP., MARKETS FOR CYBERCRIME TOOLS AND STOLEN DATA: HACKER'S BAZAAR, at ix (2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

[23] Matthew Finifter, Devdatta Akhawe & David Wagner, *An Empirical Study of Vulnerability Rewards Programs*, 22 USENIX SECURITY SYMP. 273, 273 (2013), https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/finifter.

[24] David McKinney, *Vulnerability Bazaar*, 5 IEEE SECURITY & PRIVACY 69, 69 (Dec. 12, 2007).

including both monetary rewards and recognition.[25] In some cases, third party security vendors will set up VRPs for companies that do not offer incentives to report vulnerability information. For instance, in 2007 VeriSign offered monetary rewards for exploits found in the newly released Windows Vista operating system since at the time Microsoft did not offer a VRP.[26]

Vulnerability reporting resulting in patches serves a robust preventative function. However, coordination challenges, and the lack of uniform policy regarding the public release of information about vulnerabilities, can detract from its utility. For instance, if a reported vulnerability impacts multiple vendors, it is challenging to coordinate and accommodate patch times for the many organizations that may also be competitors.[27] In addition, vendors' incentives to patch are not as straightforward as they might seem. Acting to patch vulnerabilities comes with economic tradeoffs for the affected company. When a vulnerability is made public—even where accompanied by a patch—a vendor risks facilitating more reverse engineering on its products, which makes its software potentially more vulnerable.[28] Patching can also be disruptive for end users, so even when companies issue patches, users may not apply them.[29]

b) Sharing Information About Best Practices

Regulatory models and government and private institutions facilitate sharing information about cybersecurity best practices, policies, and procedures. Regulatory models that formally adopt, or refer to, industry-

[25] Finifter et al., *supra* note 23, at 273; Sharon Solomon, *11 Essential Bug Bounty Programs of 2015*, TRIPWIRE (Feb. 10, 2015), http://www.tripwire.com/state-of-security/vulnerability-management/11-essential-bug-bounty-programs-of-2015/.

[26] Brad Stone, *A Lively Market, Legal and Not, for Software Bugs*, N.Y. TIMES (Jan. 30, 2007), http://www.nytimes.com/2007/01/30/technology/30bugs.html.

[27] Hasan Cavusoglu et al., *Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge*, 33 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 171, 171 (2007).

[28] Jay Pil Choi, Chaim Fershtman & Neil Gandal, *Network Security: Vulnerabilities and Disclosure Policy*, 58 J. IND. ECON. 868, 868 (2010). There are also alternative ways to report information like bug tracking systems that automatically facilitate the information exchange between users and vendors by reporting glitches and bugs, though the effectiveness of these systems varies depending on the design. *Towards the Next Generation of Bug Tracking Systems*, 2008 IEEE SYMP. VISUAL LANGUAGES & HUMAN-CENTRIC COMPUTING 82 (2008).

[29] For instance, a recent study of the Heartbleed vulnerability noted that the number of patches deployed plateaued after two weeks, and that 3% of the Alexa Top One Million websites were still vulnerable two months after the disclosure. Zakir Durumeric et al., *The Matter of Heartbleed*, 2014 INTERNET MEASUREMENT CONF. 475, 475, http://conferences.sigcomm.org/imc/2014/papers/p475.pdf.

generated security standards indirectly encourage information sharing about security practices. One study suggests that involving private entities in the rule-making process through regulatory delegation models may have some positive impact on security outcomes.[30] This positive impact may be a result of the increased information sharing among companies promoted by the standard development process.

Incident response organizations designed to coordinate action or facilitate a response to a security compromise also advise entities on recommended security practices to reduce cyber vulnerability. The first CERT center was established in 1988 at Carnegie Mellon University (CMU).[31] US-CERT works with a spectrum of partners (e.g., from academia, industry, ISACs, security venders, and state, local, or federal governments) and disseminates relevant threats and vulnerability information to targeted parties both large and small—from government, private sector, and the general public—in addition to their role in response management and coordination discussed below.[32] US-CERT publishes "Recommended Practices" to its website to encourage early implementation of known practices and configurations that would reduce the potential for an attack.[33] Additional CERTs operate internationally to provide complementary services, including setting standards, best practices, and policies across the world.[34] There are other federal efforts focused on improving artifacts, policies, and information sharing practices, including InfraGard[35] and the Secret Service Electronic Crimes Task

[30] David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287 (2014).

[31] The original CERT at Carnegie Mellon University is now referred to as CERT Coordination Center (CERT/CC) and works closely with US-CERT, which was established in 2003 and is a part of the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC). Stuart Madnick, Xitong Li & Nazli Choucri, *Experiences and Challenges with Using CERT Data to Analyze International Cyber Security* 2, 5 (MIT Sloan Sch. of Mgmt. Working Paper CISL #13, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478206.

[32] Gregory B. White & D.J. DiCenso, *Information Sharing Needs for National Security*, 38 HAW. INT'L CONF. ON SYS. SCI. 1, 5 (2005).

[33] *Recommended Practices*, INDUS. CONTROL SYS. CYBER EMERGENCY RESPONSE TEAM (ICS-CERT), https://ics-cert.us-cert.gov/Recommended-Practices (last visited Aug. 23, 2015).

[34] Madnick, Li & Choucri, *supra* note 31, at 2.

[35] InfraGard is a nonprofit organization and public/private partnership between the FBI and private sector to facilitate the exchange of information in order to prevent hostile threats against the United States. INFRAGARD, https://www.infragard.org (last visited July 20, 2015).

Forces (ECTF).[36] These organizations, like the CERTs, share best practices in addition to information regarding emerging threats and existing risk.

c) Sharing Information About Threats and Risks

Information sharing collaborations between industry partners are another vital way to share knowledge about threats and risks as well as preventative measures. In 1998, Presidential Decision Directive 63 (PDD-63) identified distinct industries and called for the private sector within these industries to set up ISACs to share information to mitigate risk and promote effective responses to adverse events, including cyber events.[37] For example, there is an Information Technology ISAC (IT-ISAC)[38] and a Financial Services ISAC (FS-ISAC).[39] Organizing around industry sectors facilitates more specific information exchanges about vulnerabilities, threats, and isolated incidents. There are potential risks associated with exchanging security information, such as loss of competitive advantage, market share, or stock market value from negative publicity if information is inadvertently shared with competitors or the public. However, members benefit from industry-specific information exchanges that assist in prevention efforts and vulnerability identification and management.[40]

There are several privately organized cybersecurity threat information sharing platforms (often between market competitors) like McAfee's Cyber Threat Alliance[41] and Facebook's ThreatExchange.[42] There, the information exchange may not be explicitly linked to collective action

[36] The Secret Service ECTF was created to form a network of diverse stakeholders (law enforcement, prosecutors, private industry, academics, etc.) for prevention, detection, mitigation, and investigation of cyber incidents. *Investigation*, SECRET SERVICE, http://www.secretservice.gov/investigation (last visited Oct. 18, 2015).

[37] Presidential Decision Directive 63 on Critical Infrastructure Protection, 63 Fed. Reg. 41804-01 (Aug. 5, 1998); *see also* Daniel B. Prieto, *Information Sharing with the Private Sector: History, Challenges, Innovation, and Prospects*, *in* SEEDS OF DISASTER, ROOTS OF RESPONSE: HOW PRIVATE ACTION CAN REDUCE PUBLIC VULNERABILITY 404, 406 (July 14, 2006).

[38] *Member ISACs*, NAT'L COUNCIL OF ISACS, http://www.isaccouncil.org/memberisacs.html (last visited Oct. 18, 2015).

[39] FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER, https://www.fsisac.com (last visited Oct. 18, 2015).

[40] Gal-Or & Ghose, *supra* note 16, at 187.

[41] *See* Vincent Weafer, *McAfee Founds Cyber Threat Alliance with Industry Partners*, MCAFEE LABS (Sept. 29, 2014), https://blogs.mcafee.com/mcafee-labs/mcafee-founds-cyber-threat-alliance-industry-partners.

[42] *See* Cade Metz, *Facebook Unveils Tool for Sharing Data on Malicious Botnets*, WIRED (Feb. 11, 2015), http://www.wired.com/2015/02/facebook-unveils-tool-sharing-data-malicious-botnets.

against threats and may only pertain to a narrow type of threat information—like spam propagation on spoiled URLs in ThreatExchange's case.[43] Though these alliances often consist of only a few industry members, sharing information against common threats mutually increases the value and security of their respective security software and social media platforms.

Information sharing about emerging and existing threats and risks within an industry, particularly before they have been successfully exploited, can bolster prevention-related activities. Once these vulnerabilities are exploited, information sharing assists in coordinating action to manage the resulting insecurity.

2. *Information Sharing to Manage and Respond to Vulnerabilities and Threats*

Cybersecurity must manage residual insecurity by identifying both known and unknown threats and quickly mobilizing a response that contains and treats infected systems. In addition to improving artifacts, policies, and practices in order to further preventative cybersecurity measures, US CERT Coordination Center (CERT/CC),[44] ISACs, and Secret Service ECTFs all play roles in managing the exchange of information necessary to coordinate responses to cyber incidents.[45]

There are notable cases within cybersecurity where ad hoc groups of researchers coalesced to respond to an emerging threat. Technical ad hoc working groups of researchers and practitioners self-organized to respond to the 2008 emergence of an aggressive worm (dubbed "Conficker") intended to create a botnet. Individuals from Microsoft, ICANN, domain registry operators, anti-virus vendors, and academic security researchers spontaneously formed the Conficker Working Group (CWG) to contain its spread and effectiveness.[46] Other botnet working groups, like the DNS Changer Working Group (DCWG) and the 2010 Mariposa working group, have followed the example of CWG, facilitating coordination and

[43] *ThreatExchange*, FACEBOOK, https://developers.facebook.com/products/threat-exchange (last visited Aug. 23, 2015).

[44] US-CERT, *supra* note 20.

[45] Lawrence A. Gordon, Martin P. Loeb & William Lucyshyn, *Sharing Information on Computer Systems Security: An Economic Analysis*, 22 J. ACCT. & PUB. POL'Y 461, 463 (2003).

[46] THE RENDON GROUP, CONFICKER WORKING GROUP : LESSONS LEARNED CONTRACT, at ii (2010), http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf.

information exchange.[47] Similarly, Microsoft initiated a working group in 2012 led by the Microsoft Digital Crimes Unit (with additional support from Microsoft's Malware Protection Center, the FS-ISAC, and Electronic Payments Association) to orchestrate the seizure of the Zeus botnet.[48] These working groups coordinate to varying degrees with law enforcement.[49]

Though these working groups have succeeded, by some measure, in managing coordinated responses to threats, the Conficker retrospective report recommends "improve[d] cooperation between the private sector and the U.S. government and governments around the world so that information sharing and efforts become a two-way exchange" to improve future outcomes.[50] The report also calls for clarification on the private sector's relationship with law enforcement, and procedures for reporting early warning signals to the government.[51]

Researchers have noted other weaknesses in the cybersecurity information sharing landscape including difficulty obtaining data in a timely and consistent format,[52] organizational and policy challenges associated with the dissemination of vulnerability disclosures,[53] and inattention to the privacy risks associated with sharing relevant data.[54]

Current information sharing activities attest to the various ways information can address public good challenges to cybersecurity. Today, the exchange of various kinds of information supports system improvement, shared understandings of risks, coordinated action, and priority setting. But these efforts have arisen outside a comprehensive

[47] Andreas Schmidt, *Hierarchies in Networks: Emerging Hybrids of Networks and Hierarchies for Producing Internet Security*, *in* CYBERSPACE AND INTERNATIONAL RELATIONS 181, 190–91 (Jan-Frederik Kremer & Benedikt Müller eds., 2013), http://link.springer.com/10.1007/978-3-642-37481-4.

[48] *Id.* at 191.

[49] *Id.* at 190; Milton Mueller, Andreas Schmidt & Brenden Kuerbis, *Internet Security and Networked Governance in International Relations*, 15 INT'L STUD. REV. 86, 96 (2013) ("In cases like CWG, law enforcement, intelligence agencies, and entities like CERT played a negligible role in containment. This further underscores the need for a cohesive cybersecurity response management strategy.").

[50] THE RENDON GROUP, *supra* note 46, at iv.

[51] *Id.*

[52] *See* Oscar Serrano, Luc Dandurand & Sarah Brown, *On the Design of a Cyber Security Data Sharing System*, 2014 ACM WORKSHOP ON INFO. SHARING COLLABORATION SECURITY 61, 61.

[53] *See* Jennifer Granick, *The Price of Restricting Vulnerability Publications*, 9 INT'L J. COMM. L. & POL'Y (SPECIAL ISSUE) 1, 5 (2005).

[54] *See* Gina Fisk et al., *Privacy Principles for Sharing Cyber Security Data*, 2015 IEEE INT'L WORKSHOP ON PRIVACY ENGINEERING 1, 1 (2015).

framework—such as the Doctrine for Public Cybersecurity—and thus appears as a set of loosely aligned activities rather than an integral component of a strategic, cohesive agenda. The somewhat ad hoc development of the information sharing environment, and mixture of public and private actors, has limited systematic, public consideration of their independent and collective impact on other public values. This in turn has fueled public concern about the impact of information sharing on privacy, freedom of expression, and human rights.

III. LEARNING FROM PUBLIC HEALTH

The current cybersecurity information sharing ecosystem supports activities aligned with public cybersecurity goals. Yet, these activities have emerged in a piecemeal and sporadic manner, lacking a strong vision of the potential role information sharing could play in advancing public priorities and a framework to ameliorate their impact on other values. Information sharing activities in the more mature public health domain, which address similar public goods challenges, offer insight into how a developed and coordinated information sharing system between diverse stakeholders can advance public cybersecurity goals and protect other public values.

Information sharing is pervasive in the field of public health. It plays an essential role in promoting two key public health goals: advancing the health of the population by addressing the fundamental causes of disease; and preventing adverse health outcomes in a manner that enhances the physical and social environment while respecting the rights of individuals.[55] Furthermore, the public health field has developed policies and mechanisms to balance competing values that arise in information sharing activities.

Below we discuss differences and similarities between the public health and cybersecurity domains that could affect the utility of similar activities in the realm of cybersecurity, and examine information sharing activities and their role in advancing public health functions within the field.

A. ESTABLISHING THE PUBLIC HEALTH AND CYBERSECURITY ANALOGY

The Doctrine of Public Cybersecurity differentiates between population level goals and individual responses to threats and security

[55] *See* PUBLIC HEALTH LEADERSHIP SOCIETY, PRINCIPLES OF THE ETHICAL PRACTICE OF PUBLIC HEALTH: VERSION 2.2 (2002), http://phls.org/CMSuploads/Principles-of-the-Ethical-Practice-of-PH-Version-2.2-68496.pdf.

incidents, understanding that due to its public goods characteristics, the interests of individuals, firms, and investors are not aligned to deliver an acceptable level of cybersecurity. The analogous field of public health responds to a similar problem. Public health focuses efforts at the population level—aiming to improve the functioning and longevity of the population by addressing underlying health issues and causes. Public health initiatives focus primarily on population-level responses to health concerns rather than the course of treatment for any one individual's care. While individual health choices may advance the overall health of the population, at times the interests of the population and those of the individual are misaligned, or even at odds. In such instances, the government steps in to prompt or take actions that support the overall well-being of the population. Public health has developed mechanisms for balancing the tension between individual and collective interests in such instances.

Some have expressed reservations about the analogy between cybersecurity and public health.[56] Reservations include the prominence of the intelligent sentient adversary in cybersecurity, the complexity and severity of the tradeoffs given the expressive nature of some of the information subject to sharing, the large role of the private sector given its ownership and control of relevant infrastructure and possession of relevant data, and the mixed motives of the government, which has both a defensive and an offensive interest in cybersecurity.[57] Acknowledging that there are certainly limitations to the analogy, we believe they are more in quality than in kind. For example, while pathogens may not be intelligently adversarial—as we narrowly define intelligence—biologically they evolve in form and function to adapt to environmental changes or take advantage of changing social structures (e.g., rapid spreading through urbanization, or growing antibiotic resistance from prescription overuse).[58]

[56] For example, consider the audio from the Q&A from the symposium presentation. *Panel 3: Comparative Approaches: Privacy Law and Public Health Law*, 19TH ANN. BCLT/BTLJ SYMP. (2015), https://www.law.berkeley.edu/centers/berkeley-center-for-law-technology/past-events/april-2015-the-19th-annual-bcltbtlj-symposium-open-data-addressing-privacy-security-and-civil-rights-challenges/program.

[57] *Id.*

[58] Scholars have used biological pathogens as a comparative model for phenomenon within cyberspace since the early days of networked computers. Fred Cohen used the term "computer virus" in 1983 to describe the spread and replication of malicious code in the laboratory and wild. *History of Viruses*, NAT'L INST. OF STANDARDS & TECH. COMPUTER SECURITY RESOURCE CTR. (Mar. 10, 1994), http://csrc.nist.gov/publications/nistir/threats/subsubsection3_3_1_1.html; FRED COHEN, COMPUTER VIRUSES—THEORY AND EXPERIMENTS (1984), http://web.eecs.umich

While biologically designed to survive, rather than a desire to maximize damage, the evolution that results yields an arms race that is a hallmark feature of cybersecurity. Further many cybersecurity threats like the perfunctory propagation of malware lacks sentience once released into the wild much like many biological threats. Thus while some motives vary, in both domains the public good is subject to a constantly changing battlefield of new vulnerabilities, new exploits, and wily, motivated adversaries.

More importantly, the focus on the adversarial difference often blinds us to the fact that preventative techniques are effective regardless of motive. Preventative techniques reduce vulnerabilities regardless of adversarial goals. This can be seen in public health examples such as condom use. While the intentional spreading of disease is relatively uncommon, there are instances where individuals have knowingly exposed others to HIV.[59] This intent to infect is atypical in public health, but condoms are an effective preventative measure regardless of the host's intent. Similarly, crimeware, which can be purchased en masse on the black market, is only successful if there are unpatched vulnerabilities in web applications, or if users download attachments in suspicious emails. Preventative techniques that patch vulnerabilities or limit downloads and executables are effective against exploits regardless of the enhanced abilities resulting from automation coupled with malicious intention. Adversarial considerations are simply less relevant when dealing with prevention and management orientations—in contrast to deterrence-

.edu/~aprakash/eecs588/handouts/cohen-viruses.html. Consequently words like hosts, infection, and network health have entered the cybersecurity lexicon. This biological analogy has been extended to distributed security in cyberspace, comparing its diversity to the natural ecosystem and complex system responses to the human immune system. *See* U.S. DEP'T OF HOMELAND SECURITY, ENABLING DISTRIBUTED SECURITY IN CYBERSPACE: BUILDING A HEALTHY AND RESILIENT CYBER ECOSYSTEM WITH AUTOMATED COLLECTIVE ACTION 8 (2011), https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf. Given the precedent of using biological pathogens and immune system defenses as a comparative model for cybersecurity, the comparison between public health and public cybersecurity as public goods is particularly apt.

[59] *See* Mary D. Fan, *Sex, Privacy and Public Health in a Casual Encounters Culture*, 45 U.C. DAVIS L. REV. 431 (2011). Prosecution in the United States differs by jurisdiction, and different states criminalize different behaviors specific to the knowing transmission or exposure of HIV. Philip B. Berger, *Prosecuting for Knowingly Transmitting HIV is Warranted*, 180 CAN. MED. ASS'N J. 1368 (2009), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2696543; Michael E. Miller, *Man Who Knowingly Spread HIV Sentenced to Six Months. Judge Calls it a 'Travesty,'* WASH. POST (May 5, 2015), http://www.washingtonpost.com/news/morning-mix/wp/2015/05/05/man-who-knowingly-spread-hiv-sentenced-to-six-months-judge-calls-it-a-travesty.

oriented strategies that are focused on intent—because harms manifest, and protections work, regardless of intent.

Though the implications of public health and cybersecurity data sharing are different in some instances, the individual liberties and private sector interests intruded upon are significant in both contexts. Public health initiatives at the extreme interfere with freedom of movement—for example quarantines—and bodily integrity with forced treatment for recalcitrant patients with highly contagious diseases.[60] Public health information sharing at times divulges intimate health information—including data about sexual practices, sexual partners, and drug use—to health officials, and in some instances others who are at risk of infection. Such sharing intrudes on individual privacy, questions the sanctity of the doctor-patient relationship, reveals intimate associations, and places burdens on private health care providers. Public cybersecurity information sharing activities—depending upon the information being shared—may reveal private communications, associational interests, the physical whereabouts and movements of individuals, and other personal details, and they may also disclose confidential information about companies' networks and policies.

Much of the data under discussion in the cybersecurity information sharing debates is held by the private sector. The sharing of such data may impose direct administrative costs on firms, as well as create risks to their competitiveness by forcing firms to reveal internal practices and strategies, and market reputation. This is true in the field of public health as well. Much of the data that fuels public health initiatives comes from private entities, and some are collected and sold by private organizations (e.g., insurance companies). Although there are public good benefits derived by sharing such data with the government, there are proprietary interests at stake too.

Finally, there are multifaceted, sometimes competing, national security concerns in both domains. Concerns about bioterrorism at times lead the government to limit the sharing of detailed health vulnerabilities, scientific information (i.e., viral structure and information that could allow for artificial replication),[61] or information relating to research, stockpiles, or

[60] For instance, Directly Observed Therapy (DOT) may be used as a compulsory compliance-enhancing strategy when highly infectious individuals have a history of non-compliance. LAWRENCE GOSTIN, PUBLIC HEALTH LAW: POWER, DUTY, RESTRAINT 417 (2d ed. 2008).

[61] Denise Grady & William J. Broad, *Seeing Terror Risk, U.S. Asks Journals to Cut Flu Study Facts*, N.Y. TIMES (Dec. 20, 2011), http://www.nytimes.com/2011/12/21/health/fearing-terrorism-us-asks-journals-to-censor-articles-on-virus.html.

response preparation activities—although it could be useful for public health purposes.[62] Again, this parallels the cybersecurity environment where the government is both pressing for greater information sharing to improved cybersecurity and seeking an informational advantage to support offensive cyber activities.

Like all analogies, the one between public health and public cybersecurity has limitations. However, we maintain that many of the objections to the analogy are more limited and nuanced than they first appear, and that regardless, the analogy provides important lessons about the potential benefits of cybersecurity information sharing and the conditions and mechanisms for its success. From this foundation we can better consider the role information sharing can play in supporting public cybersecurity goals, and better envision the robust protections and governance models necessary to support it in a manner consistent with other values.

B. THE ROLE OF INFORMATION SHARING IN PUBLIC HEALTH

Public health is facilitated by a wide range of interventions at the local, state and federal level, many of which are fueled by data. Data informs and makes possible many of the activities necessary to advance public health including: (1) preventing the spread of diseases, epidemics, injuries, and protecting against environmental hazards; (2) promoting healthy behaviors; (3) responding to health incidents and environmental hazards, and assisting communities during recovery; and (4) assuring the quality and accessibility of public health services.[63] All are supported by research, which requires data on population level health and disease that informs the activities in each domain.

In considering the role of information sharing in the public health—and later cybersecurity—context, it is useful as seen in Table 1 to align information sharing with particular activities under two large strategic goals: (1) prevention, which includes promoting healthy behaviors, and (2) management and response.

[62] There is also a long history of nation states developing and using biological and chemical agents offensively, which adds to potential national security concerns about information sharing from the government's perspective. *See* W. Seth Carus, *The History of Biological Weapons Use: What We Know and What We Don't*, 13 HEALTH SECURITY 219, 239 (2015).

[63] *See The Public Health System and the 10 Essential Public Health Services*, CDC, http://www.cdc.gov/nphpsp/essentialservices.html (last updated May 29, 2014).

Reviewing the role of information sharing in meeting public health goals helps clarify the potential roles information sharing could play in advancing public cybersecurity.

Table 1: Goals and Associated Activities and How They Relate to Information Sharing

	Preventative Orientation (Reducing Vulnerabilities)	Response Orientation (Managing Insecurity)
Essential public health/public cybersecurity activities (Essential public good production activities)	• Improving artifacts • Community and individual empowerment • Policy development	• Detection • Identification • Containment • Treatment
	← Ongoing Research Activities →	
Role of Information	• Program evaluations for efficacy • Inform changes to laws, regulation, architecture, and programs • Educate public	• Disease or symptom surveillance • Investigate outbreaks • Contact tracing and spread of disease • Decisions regarding future preventative activities

1. Prevention

In public health, vaccine programs, institutionalizing sanitation infrastructure, occupational hazard laws, behavioral regulations such as seatbelt laws, education, and behavioral incentive programs reduce susceptibility to disease and injury. Information is collected and shared to examine scientific and cultural or structural artifacts that introduce public health vulnerabilities within the population and particular communities. Preventative efforts include public education, community empowerment, artifact improvement, and policy development such as the creation of vaccine programs. All of these activities benefit from basic research to understand causes and effective methods[64] and are further informed by project evaluation, both of which require data collection and sharing. The ability to share data between distributed public health actors enables and sustains coordinated actions—for example, allowing public education initiatives to focus on particularly at-risk populations, or widely disseminating particularly effective interventions.

[64] *Id.*

2. *Management and Response*

Public health activities also identify and manage the constantly changing landscape of disease. Doing so requires monitoring occurrences of disease, providing information to healthcare practitioners and individuals, and, where possible, eradicating root causes of disease. Disease eradication is almost never achieved,[65] so even mitigated health threats may return. Viruses like influenza evolve over time, and rare avian and swine strains may cross over and become capable of human-to-human transmission, which introduces new threats that must be detected and identified among other common influenza strains.[66]

Management and response are information intensive public health activities. While nearly all public health activities benefit from data that can inform interventions and assist in program evaluation, disease detection presents particularly intense information demands. Whether it is monitoring the level and spread of well-known infections—such as HIV—or identifying early signs of a new virus, public health relies on a massive and distributed disease surveillance infrastructure. National data surveillance systems are an important component of the public health information sharing ecosystem, especially within management and response. Centers for Disease Control and Prevention (CDC) officials define public health surveillance as the "systematic, ongoing collection, management, analysis, and interpretation of data followed by the dissemination of these data to public health programs to stimulate public health action."[67] The purposes of health surveillance systems are made clear to justify them and distinguish them from other data collecting activities. For example, the CDC National Center for Chronic Disease Prevention and Health Promotion states that it engages in surveillance activities to: (1) understand risk behaviors, preventive care practices, and the burden of selected chronic diseases; (2) monitor the progress of current prevention efforts; and (3) inform policy and public health decisions.[68]

Health data surveillance assists in detecting vulnerabilities and vectors of disease—for example, the source of a food-borne illness—and new

[65] *See* Richard J. Whitely, *Smallpox: A Potential Agent of Bioterrorism*, 57 ANTIVIRAL RES. 7, 8 (2003).

[66] *H5 Viruses in the United States*, CDC, http://www.cdc.gov/flu/avianflu/h5/index.htm (last updated Aug. 5, 2015).

[67] Stephen B. Thacker, Judith R. Qualters, & Lisa M. Lee, *Public Health in the United States: Evolution and Challenges*, 61 CDC MORBIDITY & MORTALITY WKLY. REP. (SUPP.) 3, 3 (July 27, 2012), http://www.cdc.gov/mmwr/pdf/other/su6103.pdf.

[68] *Chronic Disease Prevention and Health Promotion: Statistics and Tracking*, CDC, http://www.cdc.gov/chronicdisease/stats (last visited May 20, 2015).

threats—such as novel virus strains—but the data collection necessary to support these activities can be quite detailed and invasive. Mechanisms and policies to balance values and tradeoffs are of the utmost importance; otherwise individuals, or the health care providers who serve them, may take evasive measures to limit the collection of sensitive information. Such evasive measures would jeopardize the overall benefits derived from this surveillance. The data garnered by public health surveillance systems are foundational to essential public health activities. A response orientation depends upon event detection and threat identification. These activities directly benefit from coordinated data surveillance activities. Data surveillance has successfully identified otherwise invisible threats like the spoiled vaccine source causing poliomyelitis in 1955 and novel infections like SARS corona virus and variants of influenza.[69] Though we consider the activities enabled by public health surveillance to fall under management and response, information generated by these ongoing activities feeds future preventative efforts and programs. Data about program effectiveness or changes within the security ecosystem fuel better prevention mechanisms through improved education efforts, program improvement, and the formation of more targeted policies.[70]

Modern public health initiatives rely heavily upon data generated by active and passive[71] public health surveillance systems,[72] which depend on widespread and systematic information sharing. Data surveillance within public health occurs at many levels with varying degrees of specificity. The collection of public health and disease surveillance information in the United States is largely conducted at a state level, but data are often shared at the national level to facilitate consideration across the larger population.[73] Surveillance may be of specific chronic conditions or

[69] GOSTIN, *supra* note 60, at 290.

[70] *The Public Health System and the 10 Essential Public Health Services*, *supra* note 63.

[71] Passive surveillance is characterized as information reported to public health agencies by healthcare providers or laboratories, whereas active surveillance involves the solicitation of information by public health officials from healthcare providers or laboratories. Contact tracing (identifying others an infected individual may have contracted an illness from or spread the illness to) is a common active surveillance practice. RUTH GAARE BERNHEIM ET AL., ESSENTIALS OF PUBLIC HEALTH ETHICS 98 (2013).

[72] There is a famous quote by U.S. Surgeon General Dr. David Satcher (1998–2002) in which he says "In public health, we can't do anything without surveillance. That's where public health begins." *Id.* at 99.

[73] There are notable exceptions, including many federally administered surveys. However, many national databases originate from state-run, cooperative programs. *See Summary of NCHS Surveys and Data Collection Systems*, CDC, http://www.cdc.gov/nchs/

infectious diseases, or may be at a more general level of capture like morbidity and birth data (also known as vital statistics). Surveillance may also be behavior specific. The CDC administers the Behavioral Risk Factor Surveillance System (BRFSS), which operates a voluntary telephone survey examining health-related risk behaviors, chronic health conditions, and use of preventative services.[74]

Data surveillance systems aim to produce consistent data over time, thus enabling historical study and comparison. These systems are uniquely situated to provide vital information for preventative efforts and programmatic decision-making, but they also fuel most of the response-oriented activities (detection, identification, containment, and treatment). The systematic collection of morbidity data across states is attributed to reducing the window of identifying incidents of natural and man-made disease. For example, the morbidity and case clusters of unusual pneumonia and rare cancers in 1981 led to the discovery of AIDS.[75]

The information shared to support these public health activities varies. Some collected and shared information presents little risk to other values. For example, the CDC coordinates PulseNet,[76] a network of state and local laboratories that analyzes the DNA fingerprints of bacteria that cause gastrointestinal infection, often associated with food-borne illness. PulseNet helps coordinate outbreak detection by creating a tailored information sharing program with minimal impact on privacy or other values. When a patient seeks medical care for severe food poisoning, healthcare providers take a fecal sample and send it to a network lab for analysis. By profiling the DNA of the underlying cause of infection (bacteria) and registering these data on a shared database, epidemiologists are able to track outbreaks or identify the source of food contamination and possibly initiate a product recall.[77] When a serious epidemic is detected, the CDC works with local and state public health officials to stop the spread and make announcements to the public about the incidents. This was recently demonstrated when drug-resistant *Shigella*

data/factsheets/factsheet_summary.htm (last updated Mar. 6, 2015). The organization and coordination between these stakeholders are discussed below. *See infra* Part IV.B.

[74] *Behavioral Risk Factor Surveillance System*, CDC, http://www.cdc.gov/brfss/ (last updated Sept. 15, 2015).

[75] GOSTIN, *supra* note 69, at 292.

[76] *PulseNet*, CDC, http://www.cdc.gov/pulsenet (last updated Sept. 9, 2013).

[77] Only when epidemiologists and microbiologists detect unusual patterns do public health officials seek out more information related to an outbreak using personal interviews that potential sources of contaminated food. *See Frequently Asked Questions, PulseNet*, CDC, http://www.cdc.gov/pulsenet/about/faq.html (last updated July 22, 2013).

sonnei began spreading within the United States and was announced in the Morbidity and Mortality Weekly Report (MMWR) with synthesized information for the public and public health practitioners.[78]

These measures to detect, identify, and respond to outbreaks work because the CDC plays a coordinating role in the analysis of samples, in information sharing between public health officials and laboratories, and in response formulation. Responsibilities for detecting these infections are distributed among many stakeholders, but are made possible on a national scale due to federal coordination.

There are other programs that demand and share far more sensitive information, intruding more heavily on individual privacy and posing a greater risk to data subjects if information is misused. We will explore how these systems are designed in the following section.

IV. PROMOTING GOALS AND MEDIATING AMONG VALUES: INSIGHTS FROM PUBLIC HEALTH

Data sharing occurs in the context of complex commitments to other values—particularly patient privacy and maximal participation in the health care system—that are at times in tension with public health information needs. Information sharing activities, if not carefully constructed, risk undermining the accuracy and completeness of the datasets since fear of stigma or discrimination stemming from keeping identified records can discourage individuals from seeking care and thus being recorded in the first place.[79] These datasets are often crucial to tailoring and evaluating interventions, so incomplete or misleading datasets have important public health consequences. A web of ethical guidelines, laws, policies and practices mitigates these tensions.

Public health information sharing arrangements are guided by a set of ethical principles. First is a commitment to seek the information necessary to implement effective policies and programs. Second is a commitment to provide communities with information necessary to make decisions on policies or programs and to facilitate community participation and consent

[78] Anna Bowen et al., *Importation and Domestic Transmission of* Shigella sonnei *Resistant to Ciprofloxacin—United States, May 2014–February 2015*, 64 CDC MORBIDITY & MORTALITY WKLY. REP. 318, 318–20 (2015), http://www.cdc.gov/mmwr/pdf/wk/mm6412.pdf.

[79] As one example, fear of social stigma and discrimination resulting from reporting requirements has been shown to keep HIV positive individuals from initially getting tested and seeking early treatment. Margaret A. Chesney & Ashley W. Smith, *Critical Delays in HIV Testing and Care*, 42 AM. BEHAV. SCI. 1162, 1162 (1999), http://abs.sagepub.com/content/42/7/1162.full.pdf+html.

in program implementation. Third is a commitment to make information held by public health institutions available in a timely manner consistent with relevant mandates and resource constraints. Fourth is a commitment to protect the confidentiality of information that can bring harm to an individual or community, and to limit intrusions on confidentiality to instances where there is high likelihood of significant harm to the individual or others. Data sharing procedures are informed by the additional principles of accountability, stewardship, scientific practice, efficiency, and equity.[80]

Though these key principles of public health information sharing aim to support common goals, in practice they can be in tension. Seeking and making information accessible to facilitate community decision making can erode individual privacy and harm individuals or communities, for example where a community suffers economic losses due to fear of a contagious disease known to be affecting the community.[81] Systematic data collection through disease surveillance places these principles in tension too. Public health surveillance systems, in general, do not rely on patient consent to collect incident data but nonetheless take great care to protect individual privacy through policies, practices, and technical mechanisms. This practice reflects a policy decision that citizens have a social contract and duty to inform the rest of the state of where their health directly implicates the well-being of others.[82] In this context, relying on voluntary participation or even offering an "opt-out" would undermine the health of society as a whole, so privacy loss is tolerated, but mitigated.

These broad ethical guidelines shape the information sharing policies, practices and mechanisms across public health institutions. Their impact is evident in legal provisions, contractual agreements, the construction of standards and data sets, and the design of platforms that facilitate access to public health data. Below we review legal frameworks, institutional policies, and mechanisms that shape the public health information sharing environment.

[80] *See* CDC, CDC-GA-2005-14, CDC/ATSDR POLICY ON RELEASING AND SHARING DATA 5–6 (2005), http://www.cdc.gov/maso/Policy/ReleasingData.pdf.

[81] Fred Barbash, *Ebola-Stricken Liberia is Descending into Economic Hell*, WASH. POST (Sept. 30, 2014), http://www.washingtonpost.com/news/morning-mix/wp/2014/09/30/hit-by-ebola-liberia-is-descending-into-economic-hell.

[82] *See* Lisa M. Lee, Charles M. Heilig, & Angela White, *Ethical Justification for Conducting Public Health Surveillance Without Patient Consent*, 102 AM. J. PUB. HEALTH 38, 41 (2012).

We organize our review around a set of four overarching principles that we distilled from the information sharing policies and practices that have emerged under the ethical guidelines outlined above: (A) expert and collaborative decisions about data collection and governance, (B) reporting minimization and decentralization, (C) earliest de-identification, and (D) limitations on non-public health related uses, particularly limits on public record requests and law enforcement access and use. These principles facilitate effective large-scale public health information sharing activities, while protecting other values that might, if left unchecked, undermine public support for public health driven data collection, and suppress access to care, thus reducing the availability of essential data. Lastly, we review the access policies and mechanisms that support public health information sharing to explore how they influence, practice, and further promote the four core ethical principles.

Together, the principles and aligned access models provide useful guidance for cybersecurity policy and practice. Tailoring information sharing to support public cybersecurity goals, and implementing policies and mechanisms aligned with these principles, could assuage the concerns of individuals and organizations who might otherwise attempt to subvert cybersecurity data collection and sharing.

A. EXPERT AND COLLABORATIVE DECISIONS ABOUT DATA COLLECTION AND GOVERNANCE: PRACTICES, STANDARDS, AND RELEASE PROCEDURES

The capacity for public health databases and data collection and sharing mechanisms to advance public health goals depends upon their utility and interoperability, and demands coordination and data governance at a national level. However, these decisions cannot be made by federal entities alone. Public health experts develop decisions about information sharing initiatives, data elements, practices, technical standards, and the associated financial and technical burdens, along with organizational responsibilities. These decisions evolve over time to respond to emerging needs and feedback from practitioners, public officials, and the general public.

Choices about what data should be collected and at what granularity impact future public health utility and present both administrative and privacy tradeoffs. The Council of State and Territorial Epidemiologists (CSTE)[83] works directly with the CDC to determine which diseases

[83] COUNCIL OF STATE & TERRITORIAL EPIDEMIOLOGISTS, http://www.cste.org (last visited July 20, 2015).

should be included or removed from national reporting, like those included in the National Notifiable Disease Surveillance System. For federally administered surveillance surveys (e.g., BRFSS), states and public health partners are able to request new data elements or topic specific modules in order to improve the survey utility for stakeholders' public health activities.[84] Stakeholder feedback on nationally administered activities builds trust and cooperation among public health partners, and improves the utility of the survey data for research and program/initiative evaluations. Sub-committees, made up of program officers from the CDC as well as CSTE, have been convened to perform surveillance oversight and evaluation,[85] as well as create national plans for data governance like the CDC-CSTE Intergovernmental Data Release Guidelines.

At the federal level, the CDC/ATSDR Policy on Releasing and Sharing Data governs data quality, compliance, and data release and sharing.[86] The policy tasks the Chief Information Officer (CIO) with evaluating data quality and the risk of disclosing private or confidential information, and establishing obligations for non-CDC data users, grantees, contractors, and partners, among other things.[87] When assessing data quality, CIOs are required to test for completeness, validity, reliability, and reproducibility.[88] The CDC follows quality guidelines put forth by itself, Health and Human Services (HHS), and the Office of Management and Budget (OMB).[89] The HHS Information Quality Guidelines stipulate that Requests for Correction (RFC) and Requests for Reconsideration (RFR) may be submitted to HHS for review, and

[84] Amy B. Bernstein & Marie Haring Sweeney, *Public Health Surveillance Data: Legal, Policy, Ethical, Regulatory, and Practical Issues*, 61 CDC MORBIDITY & MORTALITY WKLY. REP. (SUPP.) 30, 33 (July 27, 2012), http://www.cdc.gov/mmwr/pdf/other/su6103.pdf.

[85] *See* Lisa M. Lee & Stephen B. Thacker, *The Cornerstone of Public Health Practice: Public Health Surveillance, 1961–2011*, 60 CDC MORBIDITY & MORTALITY WKLY. REP. (SUPP.) 15, 16 (Oct. 7, 2011), http://www.cdc.gov/mmwr/pdf/other/su6004.pdf.

[86] *See* CDC/ATSDR POLICY ON RELEASING AND SHARING DATA, *supra* note 80.

[87] The CIO must report the implementation to the CDC Associate Director for Science (ADS) as well. *Id.* at 10.

[88] *Id.* This requirement extends to research publications, official reports, oral presentations, and statistical information (i.e. data) put out by the CDC, but does not apply to documents authored or presented by other non-CDC parties. *Id.* at 3–4.

[89] *See Advancing Excellence & Integrity of CDC Science*, CDC, http://www.cdc.gov/od/science/quality/support/info-qual.htm (last visited May 1, 2015); OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies, 67 Fed. Reg. 8452 (Feb. 22, 2002), https://www.whitehouse.gov/sites/default/files/omb/fedreg/reproducible2.pdf. OMB often mandates the use of specific questions for surveyed variables, like sex, ethnicity, and race. Bernstein & Sweeney, *supra* note 84, at 33.

requires that these requests are posted with all documentation and status updates on the Internet for public transparency.[90] The mechanism provides recourse for those concerned with the quality of data released for public use. Requestors range from contract employees to advocacy or trade organizations and private citizens.

CDC guidelines require that data stewards review all data prior to release to assess the risks of re-identification and determine if additional steps are necessary to ensure confidentiality. This evaluation of risk points to the 18 variables considered identifiers under the Heath Insurance Portability and Accountability Act (HIPAA) that must be removed before a dataset may be considered de-identified[91]—even though the policy guidance notes that releasing public health information is not covered under HIPAA.[92] The policy notes the tension between reducing the privacy risk of disclosure, and managing the overall utility of the data for public health research and practice. The U.S. Census Bureau provides additional resources covering Statistical Disclosure Control that other agencies may adapt to minimize risks when releasing data.[93] Occasionally the CDC is unable to specify formats, delivery modes, and opportunities for data sharing and release. Pre-existing funding and cooperation agreements for surveillance activities can reduce their ability to influence data products and uses. In contrast, when a contract dictates funding, it is easier to influence and evolve the data specifications and sharing obligations, including privacy requirements, in a way that benefits public health.[94] The centralized authority from the CDC and other coordinating groups, based on stakeholder feedback, provides guidance and contract incentives to make data as open and accessible as possible while balancing privacy and sensitivity considerations.

Decisions about the release of sensitive information do not only occur at a national level. In addition to the practices described above, the National Center for Health Statistics (NCHS) (a federal entity) and the

[90] *Information Requests for Corrections and HHS' Responses*, DEP'T HEALTH & HUMAN SERVS., http://aspe.hhs.gov/information-requests-corrections-and-hhs-responses (last visited Oct. 20, 2015).

[91] CDC/ATSDR POLICY ON RELEASING AND SHARING DATA, *supra* note 80, at 11.

[92] CDC, CDC-ATSDR DATA RELEASE GUIDELINES AND PROCEDURES FOR RE-RELEASE OF STATE-PROVIDED DATA 71 (2005), http://stacks.cdc.gov/view/cdc/7563.

[93] *Statistical Disclosure Control (SDC): Documents used by the Census Bureau's Disclosure Review Board*, U.S. CENSUS BUREAU, http://www.census.gov/srd/sdc/ (last visited May 1, 2015); *see also* U.S. CENSUS BUREAU, DISCLOSURE REVIEW BOARD (2001), http://www.census.gov/srd/sdc/wendy.drb.faq.pdf.

[94] Bernstein & Sweeney, *supra* note 84, at 34.

National Association for Public Health Statistics and Information Systems (a non-profit that represents states and territories) collaboratively review researchers' data requests for restricted vital statistics files. The National Association for Public Health Statistics and Information Systems reviews the requests before the federal entity, NCHS, which allows the state data owners to share oversight with the federal government.[95] The distribution of responsibility and oversight adds an additional layer of protection and collaboration between public health stakeholders.

The CDC and the Agency for Toxic Substances and Disease Registry (ATSDR)[96] work with other public coordinating groups and periodically amend current practices and release guidance documents on data use, release, and sharing. These guidance documents clarify goals in data management and sharing practices, ensure compliance with relevant federal laws and guidelines (e.g., HIPAA, the Freedom of Information Act (FOIA),[97] OMB Budget Circular A110, and Information Quality Guidelines, etc.), and promote the routine and prompt sharing of data by the federal government with public health partners while protecting sensitive data. The data covered by federal guidance documents does not include data owned by private organizations and shared with the federal government, though these data may still fall under the jurisdiction of other laws, regulations, or agreements.[98]

Technical standards and requirements facilitate information sharing, and the protection of privacy and other values. Public health policy looks to develop voluntary consensus standards to facilitate information sharing.[99] The Public Health Information Network (PHIN) is a national initiative within the CDC Division of Health Informatics and Surveillance (DHIS) designed to increase the capacity of public health agencies to electronically exchange data and information through the establishment of standards[100] and technical requirements.[101] Most of the

[95] *Id.*

[96] The CDC and ATSDR are both under the HHS. Many of the data sharing policies were written jointly by both of these agencies since both agencies play a large role in public health data collection and dissemination. For simplicity in this paper, we will refer only to the CDC when talking about public health data sharing practices.

[97] For a discussion of FOIA, *see infra* Part IV.D.

[98] CDC/ATSDR POLICY ON RELEASING AND SHARING DATA, *supra* note 80, at 3.

[99] To develop voluntary consensus standards, the federal government fulfills requirements set forth by the National Technology Transfer Advancement Act of 1995 (NTTAA). *See generally* National Technology Transfer Advancement Act of 1995, Pub. L. No. 104-113.

[100] PHIN uses OMB Circular A-119 for their definition of "standard." *Standards and Interoperability Enterprise Services*, CDC, http://www.cdc.gov/phin/resources/

standards for public health data are directed by existing laws and policies that specify the voluntary consensus and evaluation processes, and are enumerated on the PHIN website.[102] These PHIN standards and interoperability activities are part of CDC-wide standardization activities, which the National Institute of Standards and Technology (NIST) publishes annually in the NTTAA annual reports.[103]

The CDC has a goal to make data standards and documentation compatible with those used in private industry to facilitate data use for public health purposes. Given the often rapid pace of innovation within the private sector, these standards are developed and reviewed for best practices, and the CDC recommends data documentation elements in its data sharing policy.[104]

Through collaboration across industry and government, public health officials have designed interoperable data formats, systems, and policies that improve the potential utility of information sharing activities undertaken to promote public health goals. These collaborative efforts foster trust across institutional actors and the public, and support innovation within the field. Officials are also able to attend to values such as privacy through policy measures and technical choices that affect the entire ecosystem.

B. REPORTING MINIMIZATION AND DECENTRALIZATION

Reporting minimization and decentralization are common elements of the public health data collection landscape. Legal frameworks, institutional policies and practices, and technical approaches to data sharing reflect preferences for keeping data in the hands of the initial collector rather than pooling it, and minimizing the data that flows when sharing is necessary. Adherence to these principles erects practical barriers to the misuse or repurposing of public health data at scale; multiple

standards/index.html (last updated July 1, 2015); s*ee also* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB CIRCULAR NO. A-119, REVISED, FEDERAL PARTICIPATION IN THE DEVELOPMENT AND USE OF VOLUNTARY CONSENSUS STANDARDS AND IN CONFORMITY ASSESSMENT ACTIVITIES (1998), http://www.nist.gov/standardsgov/omba119.cfm.

[101] Public Health Information Network Homepage, CDC, http://www.cdc.gov/phin/about/index.html (last updated Sept. 10, 2015).

[102] *Data Interchange Standards*, CDC, http://www.cdc.gov/phin/resources/standards/data_interchange.html (last visited May 1, 2015).

[103] Database of Reports Submitted Under the National Technology and Advancement Act of 1995, NIST, https://standards.gov/NTTAA/agency/index.cfm?fuseaction=agencyReports.main (last updated Mar. 7, 2013).

[104] CDC/ATSDR POLICY ON RELEASING AND SHARING DATA, *supra* note 80, at 3.

systems must be compromised, or multiple entities convinced for a shift in use to occur. When breaches or shifts in use occur, the limited nature of the data often reduces the potential harms. Minimization can reduce the attractiveness for abuse of the underlying data by limiting its potential for misuse or repurposing.

Much of the data used for public health purposes is not collected or held at the federal level, but rather generated, stored, and used by state, local or non-state organizations. Data obtained for public health uses come from four different types of sources: (1) data that the CDC collects directly using federal funds, (2) data that other agencies or organizations collect for the CDC (e.g., through procurement mechanisms like grants, contracts or cooperative agreements),[105] (3) data that other organizations like state health departments report to the CDC, and (4) privately collected data shared with the CDC. As discussed below, data that parties collect under federal or state authority to advance specific public health goals may only be used for these purposes.[106]

The Public Health Services Act (PHSA) authorizes federal public health data collection.[107] The government often uses federal administrative data, including Medicare, Medicaid, and Social Security Disability data, for public health surveillance purposes.[108] Many data reporting mechanisms are voluntary collaborations between data holders (often state health departments) and the federal government. While most state data reporting to the federal government is voluntary, it is conducted with federal and peer-based committee guidance via the CSTE on data collection, standardization, and compliance with state laws and regulations.[109]

When data is collected at a federal level, only data necessary to achieve public health goals are reported. Federal agencies like the CDC have their own collected datasets (like survey responses) that may include identifiable information, but these datasets are limited. There are notable emergency cases where the federal government requires identifiable data, such as in bioterrorism responses that require joint law enforcement and public health action using special information sharing protocols that comply with

[105] *Id.*

[106] Data may be used for other purposes only if the data subject gave appropriate consent at the time of collection. *See infra* Part IV.D.

[107] 42 U.S.C. §§ 242b, 242k, 242l (2012).

[108] Bernstein & Sweeney, *supra* note 84, at 32.

[109] GOSTIN, *supra* note 60, at 286–87.

all applicable laws and regulations.[110] In most cases, identifiable public health surveillance data are only maintained at the local government level (i.e., state or county) where it was obtained. Local and state laws regulate collection and confidentiality as well. These state and local entities are ultimately responsible for ensuring confidentiality protections to the data they collect and maintain.[111] This separation between collection and reporting means that most sensitive micro-data never reach the federal level, which is where the majority of data releases and sharing activities in support of public health occur.[112]

This separation between collection and federal reporting, as well as clear delineation about what micro-data are appropriate for public health uses, is vital to making these national reporting structures work while balancing the rights of individuals and the benefits for the collective. As a result, public health data is often reported in a *relatively* privacy-protective manner. Often, no identifiers and only broad regional locations are reported as summary level statistics. Though there are perennial concerns that someone can easily re-identify data when coupling with other attributes (e.g., age, geolocation, etc.), efforts to remove identifiable data, along with limited federal collection, assists in protecting the privacy of citizens. This network of information providers and targeted federal collection activities make possible the robust data available for public health activities.

C. EARLIEST FEASIBLE DE-IDENTIFICATION

At times advancing public health goals requires sharing identifiable information that allows officials to link these data to other datasets or identify persons with a specific disease or health condition. In almost all cases, these identifiable data only remain at the level where the

[110] Joint investigations between law enforcement and public health officials imply that both entities may be interviewing (and obtaining data about) potential patients, and that public health officials may need to disclose protected health information to law enforcement to avert a serious threat to health or safety as guided under 45 C.F.R. § 164.512(j) (2013). Many emergency information sharing protocols are issued at a local level to ensure that all applicable laws and regulations (including state) are complied with in a timely and orderly fashion. *See, e.g.*, L.A. CNTY. DEP'T OF HEALTH SERVICES, L.A. CNTY. SHERIFF'S DEP'T & FBI L.A. FIELD OFFICE, JOINT BIOTERRORISM INVESTIGATION MEMORANDUM OF UNDERSTANDING (2005), http://www2a.cdc.gov/PHLP/docs/joint%20mouLA.pdf.

[111] CDC-ATSDR DATA RELEASE GUIDELINES AND PROCEDURES, *supra* note 92, at 6; *see also* CDC/ATSDR POLICY ON RELEASING AND SHARING DATA, *supra* note 80, at 8.

[112] Bernstein & Sweeney, *supra* note 84, at 30.

intervention occurred, which is usually the state or local level.[113] In limited cases, such as a rare disease outbreak or certain high-risk disease surveillance programs, these local or state entities may share identifiable data with other jurisdictions or report them to federal agencies. For example, within the HIV/AIDS surveillance system, experts support the routine sharing of some data with identifiers in order resolve duplicate case counts across states and territories to assure data quality at a national level.[114]

In the cases where identifiable data must be transferred, there are polices in place to limit risk. Encryption standards and practices—such as replacing names with numbers in records and maintaining the file that connects them separately and in an encrypted format—aim to reduce the potential risk these sharing mechanisms impose.[115] However, in most cases where an organization collects identifiable data, it is de-identified as soon as possible, and before sharing occurs.

The commitment to earliest feasible de-identification plays a particularly important role in public health reporting obligations. Obtaining patient consent to share data for public health reporting would add an administrative burden to healthcare professionals, potentially slow down an already cumbersome reporting process (timeliness is particularly prized in some settings, such as when a new communicable disease is spreading), and limit reported data. Where compulsory information sharing is necessary for public health purposes, de-identification and other efforts at minimization (described above) are largely accepted as sufficient to mitigate privacy harms.[116]

Balancing potential utility with individual privacy is an ongoing struggle as data reporting needs and systems evolve. Though much of the data that is reported at a national level is de-identified to some extent, datasets have varying levels of specificity, and some may be tied to additional data that makes identification easier, such as a geographic marker of residence.[117] Geographic markers, gender, age and other data

[113] *Id.*

[114] Amy L. Fairchild et al., *Public Goods, Private Data: HIV and the History, Ethics, and Uses of Identifiable Public Health Information*, 122 PUB. HEALTH REPS. (SUPP.) 7 (2007), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1804110/pdf/phr122S10007.pdf.

[115] *Standards to Facilitate Data Sharing and Use of Surveillance Data for Public Health Action*, CDC, http://www.cdc.gov/nchhstp/programintegration/SC-Standards.htm (last updated Mar. 11, 2014).

[116] *See* BERNHEIM ET AL., *supra* note 71.

[117] COMMITTEE TO REVIEW DATA SYSTEMS FOR MONITORING HIV CARE BOARD ON POPULATION HEALTH AND PUBLIC HEALTH PRACTICE, MONITORING

increase the risk of re-identification.[118] However they may be important to understanding public health risks, assessing the efficacy of interventions, and understanding the limits of collected data. There is a notable tension between the need to protect individuals against re-identification and the need to provide public health officials, researchers, and healthcare providers with enough specificity to act or test correlative hypotheses and enough information to understand the strength and limits of their findings.[119]

D. LIMITATIONS ON NON-PUBLIC HEALTH USES THAT NEGATIVELY AFFECT INDIVIDUAL INTERESTS

Public health law provides confidentiality protections that limit the reuse of and access to data collected for public health purposes. These use and access restrictions make the intrusions on individual privacy necessary to advance collective public health goals more palatable. Institutional policies, contracts, and technical mechanisms further limit non-public health uses, particularly those detrimental to individual data subjects.

Data held by the CDC—the primary federal public health agency—is subject to the general federal laws and regulations that govern retention,

HIV CARE IN THE UNITED STATES: INDICATORS AND DATA SYSTEMS 14 (Morgan A. Ford & Carol M. Spicer eds., 2012). Within the National HIV Surveillance System, various data elements are captured through proxy indicators that are used to improve longitudinal data and make the system more robust.

[118] *See* Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* 2 (Carnegie Mellon Univ., Data Privacy Working Paper No. 3, 2000); *see also* Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, 2008 IEEE SYMP. ON SECURITY & PRIVACY 111, 111.

[119] Differential privacy, which allows researchers to receive statistically meaningful answers to queries while limiting their ability to determine whether a given individual is in or out of the data set, provides a mathematically rigorous way to specify the trade-off between privacy and utility. iDASH (Integrating Data for Analysis, Anonymization, and Sharing), which is funded by the National Institutes of Health, is developing a statistical health information release toolkit with differential privacy. *SHARE: Statistical Health Information Release with Differential Privacy*, IDASH, https://idash.ucsd.edu/share-statistical-health-information-release-differential-privacy (last visited Oct. 21, 2015). The Census Bureau is also using differential privacy. *See* Erica Klarreich, *Privacy by the Numbers: A New Approach to Safeguarding Data*, QUANTA MAG. (Dec. 10, 2012), https://www.quantamagazine.org/20121210-privacy-by-the-numbers-a-new-approach-to-safeguarding-data. The CDC states that those assessing risks associated with public health data release should recommend statistical methods to protect confidential information from being disclosed, such as "suppression, random perturbations, recoding, top- or bottom-coding." CDC/ATSDR POLICY ON RELEASING AND SHARING DATA, *supra* note 80, at 11.

access, and disclosure of personally identifiable information.[120] The CDC complies with the Federal Records Act, which governs the retention, destruction, and archiving of federal records,[121] and it sets additional rules regarding retention of data collected for public health purposes.[122] CDC policies leave local (state and municipal) data retention and destruction requirements (which may be more restrictive than federal standards) up to local agencies to ensure their own compliance after reporting to the federal government.[123] FOIA promotes government transparency and accountability to citizens by allowing individuals to request the release of agency records, and it contains nine exemptions,[124] two of which provide specific protection against the release of sensitive health information.[125] While FOIA serves an important purpose, the exceptions balance government transparency and accountability with public health goals and the privacy protections required to achieve them. The result is a policy framework that protects CDC data tied to an individual (e.g., health behavior survey response) and other sensitive datasets from FOIA release.[126] The Privacy Act of 1974 provides additional protections, preventing the disclosure of personally identifiable information contained

[120] CDC-ATSDR DATA RELEASE GUIDELINES AND PROCEDURES, *supra* note 92, at 69.

[121] 44 U.S.C. ch. 33 (2012); 36 C.F.R. ch. 12, subch. B (2009).

[122] *See, e.g.*, CDC Notice, Republication of Systems of Records, 51 Fed. Reg. 42,449, 42,460 (Nov. 24, 1986) (setting rules regarding retrieval of records collected for determining eligibility under the Tuskegee Health Benefit Program).

[123] CDC-ATSDR DATA RELEASE GUIDELINES AND PROCEDURES, *supra* note 92, at 69.

[124] Exemptions from FOIA are found under 5 U.S.C. § 552(b) (2012), which protects files related to national security, trade secrets and commercial or financial information from a person that is privileged or confidential, medical files or other similar files where disclosure would constitute a clearly unwarranted invasion of privacy, and information that is prohibited from disclosure by another federal law. The exemptions are aimed to "protect certain equally important rights of privacy with respect to certain information in Government files, such as medical and personnel records." S. REP. NO. 88-1219, at 8 (1964).

[125] 5 U.S.C. § 552(b)(6) limits the application of FOIA to "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." This has been interpreted to protect medical records. *See, e.g.*, McDonnell v. United States, 4 F.3d 1227, 1254 (3d Cir. 1993). 5 U.S.C. § 552(b)(3) limits the application of FOIA where records are specifically exempted from disclosure by another statute that leaves no discretion on the issue; or establishes particular criteria for withholding or refers to particular types of matters to be withheld; and if enacted after the date of enactment of the OPEN FOIA Act of 2009, specifically cites to this paragraph.

[126] FOIA exemptions include "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of privacy." 5 U.S.C. § 552(b)(6).

in a system of records[127] unless the individual to whom the record pertains consents, it is for a "routine use" defined as one "compatible with the purpose" of collection, or another agency requests it and it is relevant to the investigation of a specific violation of law.[128]

The PHSA provides additional privacy protections for public health data that limit the potential for data to be used in ways that negatively affect individuals.[129] The PHSA closes gaps in other federal laws to protect individuals, and, in some cases, organizations, who may be the subject or contributor of information gathered for public health purposes.[130] The CDC offers general confidentiality assurance provisions for both individuals and establishments by prohibiting the use of data collected for any other purpose than the purpose for which it was collected, unless the individual has consented to the alternative use.[131] Further, any information collected during the course of statistical or epidemiological activities may not be published or released in other form if an individual or establishment is supplying the information or described within it are identifiable, unless the individual consents.[132] Confidentiality assurances afforded under the Act protect against disclosure under a court order, and extend protections to institutions and not just individuals. This confidentiality protection allows the CDC to guarantee participants and institutions that their data will only be shared with entities listed on the consent form or Assurance of Confidentiality Statement for the project, which is especially important when data gathering includes sensitive information that otherwise might be withheld, like sexual behaviors, drug

[127] Unlike FOIA, which pertains to all federal agency records, the Privacy Act pertains only to records within a system of records in which the primary method of data access is through retrieval by full names, social security numbers, or other identifying particulars. 5 U.S.C. § 552a(4).

[128] 5 U.S.C. § 552a(b). There are additional limitations—notably the records of deceased persons or non-US citizens are not protected. *Id.*; *see also* CDC-ATSDR DATA RELEASE GUIDELINES AND PROCEDURES, *supra* note 92, at 75–77.

[129] Public Health Service Act, Pub. L. No. 78-410, 57 Stat. 682 (1944) (codified at 42 U.S.C. ch. 6A); 42 U.S.C. §§ 241(d), 242m(d).

[130] Here we focus on the protections offered at a federal level, but it should be noted that since most identifiable data are collected at the local level, state laws are highly relevant. All states offer some legal protection for government-held public health data (especially sensitive data like sexually transmitted infections or data relating to drug and alcohol treatment), but vary in their scope, specificity, and reach to protections for privately held data. It is beyond the scope of this paper to discuss the nuances and shortcomings of these laws, but we acknowledge the weaknesses this introduces into public health data privacy protections at a system level. GOSTIN, *supra* note 60, at 326.

[131] 42 U.S.C. § 242m(d).

[132] *Id.*

uses, mental health status, or other information that could damage an individuals' reputation financially or socially. These provisions cover research and non-research activities that the CDC carries out or that are under contract to the CDC.

To cover public health information activities conducted under grants or cooperative agreements, the CDC can provide Certificates of Confidentiality to a research project.[133] Certificates of Confidentiality authorize researchers to protect the privacy of individuals so that no federal, state, or local civil, criminal, administrative, legislative, or any other proceedings can compel the release of identifying information unless the individual consents.[134] Certificates cover sensitive information including research pertaining to mental health, and the use and effects of alcohol and other psychoactive drugs.

This suite of additional legal protections ensures that robust public health data collection does not undermine access to health care services and protects institutional interests implicated in data sharing. Confidentiality assurances extend not only to individuals but also institutions that may require protection in order to consider sharing data with the government. The additional Certificates of Confidentiality for activities conducted outside of the federal government allow public health officials to offer important prohibitions on otherwise compulsory uses of data (e.g., for law enforcement activities). Without these protections, researchers and public health officials would lose access to highly sensitive data like statistics related to drug-use and addiction patterns.

E. PUBLIC HEALTH INFORMATION SHARING MODELS

A rich and diverse set of information sharing models support public health goals. These models provide examples of the principles in action using specific data sharing mechanisms. Below we discuss three common models of information sharing and access that public health agencies offer. We also discuss non-governmental models for data sharing. A similar range of public sector and private approaches could advance public cybersecurity goals.

1. *Access to Federally Held Data*

The CDC operates on the premise that public health goals and scientific achievement are best promoted by releasing or sharing data in an

[133] 42 U.S.C. § 241d.

[134] CDC-ATSDR DATA RELEASE GUIDELINES AND PROCEDURES, *supra* note 92, at 77.

open, timely, and responsible way with public health agencies, academic researchers, and other private researchers.[135] Federal public health agencies—namely the CDC in the U.S.—must balance timeliness, data quality, and wide dissemination of data with the need to ensure protection of sensitive information. Sensitive information considerations within public health include protecting the privacy of individuals in the dataset, proprietary interests of data sharing partners, national security interests, and law enforcement activities (including misconduct inquiries and investigations).[136] Balancing these interests in different data sets and contexts requires different approaches.

Three general access models have emerged to support public health data sharing: (1) Open Data—no restrictions and public open access, (2) Limited access with restrictions, and (3) No Access except for internal agency use (not eligible for release or sharing). The choice of access model can depend on legal constraints, ethical guidelines discussed above, and community and public input. Here we will explore how the CDC determines and administers data access, along with the sharing mechanisms, protocols, and laws that preside over data use. These models present opportunities and considerations for handling sensitive data in the cybersecurity context.

a) Open Data: No Restrictions and Public Open Access

According to the CDC/ATSDR Policy on Releasing and Sharing Data, all data the CDC collects or holds that are legally eligible for public release should be publically available within a year of being evaluated for quality and shared with public health partners.[137] When releasing public-use data, the CDC follows procedures to ensure that data are consistent with the standards the PHIN has established.[138]

Each data set must have a specific data release plan to address data sensitivities prior to release. These plans include steps to reduce the risk of confidential information disclosure, procedures to ensure release does not interfere with national security or law enforcement activities, protections for proprietary information, a data quality analysis as required by OMB, instructions on appropriate data use for non-CDC users, timely release schedules, and data formats and standards compliance.[139]

[135] *See* CDC/ATSDR POLICY ON RELEASING AND SHARING DATA, *supra* note 80, at 1.

[136] *Id.* at 2.

[137] *Id.* at 7.

[138] *Id.*

[139] *Id.* at 8.

Data shared without restrictions may be released through the CDC Information Center, and shared through the CDC/ATSDR Scientific Data Repository and the associated data dissemination portal CDC WONDER.[140] The CDC WONDER platform offers an example of how these laws and policies come together in practice. Individuals accessing open data sets through the CDC WONDER platform are shown a brief description of the data, along with applicable use restrictions.[141] In addition to stating these restrictions, the agreement sets lower limits on sample size reporting within a set geographical region in a public dataset (i.e., datasets do not report alone nine or fewer death rates within a sub-geographic region), and makes it clear that any attempt to identify individuals within the dataset is illegal. The platform informs users that they should not further disclose any inadvertent discoveries, and that they must report these discoveries to the NCHS Confidentiality Officer with the contact information provided.[142] Researchers who are found violating the data use restrictions lose access to the CDC platform, and the researcher's institutional sponsors receive notifications about the violation. Access to CDC WONDER is denied until the government conducts an investigation. If the researcher is found to be deliberately making false statements within the jurisdiction of any department or agency of the federal government[143] they may be punished by a fine and/or up to five years in prison.[144]

In some cases, it may be appropriate to release high-level data but offer granular data under a restricted access model. In cases like the National Violent Death Survey, this process has helped improve researcher and program use of these data. Because interested parties can use higher-level data prior to submitting a request for access, they can better determine how data might fit specific needs or research questions.[145]

[140] *WONDER Online Databases*, CDC, http://wonder.cdc.gov (last visited Apr. 1, 2015).

[141] *Data Use Restrictions*, CDC, http://wonder.cdc.gov/DataUse.html (last visited Oct. 21, 2015). For example, the CDC states that data "may be used only for the purpose for which they were obtained; any effort to determine the identity of any reported cases, or to use the information for any purpose other than for statistical reporting and analysis, is against the law." *Id.*

[142] *Id.*

[143] 18 U.S.C. § 1001 (2012).

[144] *Id.*

[145] *National Violent Death Reporting System: Restricted Access Database (RAD)*, CDC, http://www.cdc.gov/violenceprevention/nvdrs/rad.html (last visited May 1, 2015).

b) Limited Access with Some Restrictions

If data cannot be shared openly with the public, the next policy option is to allow access with restrictions, or to mediate access. Data may be released with restrictions either under controlled conditions or through special-use agreements. Controlled conditions for data release can take the form of research data centers (RDCs) or licenses that limit use of accessed data for non-CDC researchers. Licenses attach these legal responsibilities, binding the external researcher before providing her access to identifiable data.[146] Prior to entering into a special-use agreement, the CDC screens requests to ensure the use is for an appropriate public health purpose.[147]

RDCs offer different access modes, which are not mutually exclusive (a researcher may use a combination of access modes). Researchers interested in using restricted use data must submit a proposal requesting one or more access modes, which include visiting a center[148] or gaining remote access. Approved researchers can remotely query some restricted use datasets held by an RDC. Researchers submit code through an automated system that analyzes the restricted data and returns results. There are technical limitations to these options at the CDC (a researcher can only run some SAS/SAS-callable SUDAAN procedures), for researchers who must use secure email addresses, and for research teams—only one researcher per team can have remote access rights.[149] In addition to time restrictions, research protocols are subject to RDC analysts performing disclosure reviews of the SAS code and output.[150] Any violation or attempt to circumvent remote access protocol to obtain access to prohibited information results in immediate account suspension and potential legal actions. If this method does not meet the researcher's needs, it is possible to apply for staff assisted access, where an RDC analyst runs a set of programs that the researcher created and provides the results separately.

[146] CDC/ATSDR POLICY ON RELEASING AND SHARING DATA, *supra* note 80, at 9.

[147] *Id.*

[148] Researchers may choose between a National Center for Health Statistics (NCHS) RDC (which has three locations in MD, GA, and DC) or Federal Statistical RDCs (which have over 19 locations and are managed by the U.S. Census Bureau). If researchers use a Federal Statistical RDC, a NCHS RDC analyst still handles the proposal and all administrative concerns, and the Census RDC Centers only serve as an access facility. *On Site at a Federal Statistical RDC*, CDC, http://www.cdc.gov/rdc/b2accessmod/acs220.htm (last visited May 1, 2015).

[149] *Remote Access*, CDC, http://www.cdc.gov/rdc/b2accessmod/acs230.htm (last visited May 1, 2015).

[150] *Id.*

If allowed, sensitive data may be released under special-use agreements outside the controlled conditions of an RDC. These agreements address co-authorship, but more importantly for this discussion, they provide for the CDC to review all findings resulting from restricted data use, review publications, and establish a time when researchers must return data. In order to be eligible for a special-use agreement, the research must be necessary for a legitimate public health purpose. The agreement must contain a list of data use restrictions, names of all researchers with access to the data, information regarding pertinent laws relating to the use of the data, security procedures and associated penalties for failure to comply, a list of restrictions on releasing data analysis results, procedures for data return to the CDC and managing access of staff changes, and provisions to cover emergency requests for identifiable or confidential data.[151]

These public health procedures and policies, which offer full and access-mediated release of data to promote public good activities, balance data sensitivity concerns with the benefits of open data access. By not restricting access to a binary all-or-none model, public health policy is able to optimize data sharing and use without compromising privacy and security interests.

c) Internal Agency Use Only

One of the core principles within public health information sharing is to make data as accessible as possible with the minimum amount of restrictions necessary to protect individuals and organizations.[152] If the government does not release data, the conclusion is that public use or mediated access modes were not appropriate. Despite the preference for robust access to support public health uses, at times other values council against sharing. Reasons to withhold data may include, but are not limited to: data classified for national security reasons, proprietary data from non-governmental organizations, and identifiable or particularly sensitive data.

The varied role the federal government plays in public health information and data governance, the nuanced options for data access that protect sensitivities while promoting openness and accessibility, and the different approaches to data platform operations, together provide a set of policy and organizational offerings that can be applied to public cybersecurity.

[151] CDC-ATSDR DATA RELEASE GUIDELINES AND PROCEDURES, *supra* note 92, at 29–31.

[152] *See* CDC/ATSDR POLICY ON RELEASING AND SHARING DATA, *supra* note 80, at 2.

2. *Non-Governmental Platforms for Public Health Information Sharing*

In addition to the CDC WONDER platform, there are information sharing platforms managed by non-governmental organizations that operate with limited federal funding and coordination. For example, the BioSense program is a streamlined collaborative data-exchange system that allows users (public health officials in cooperating jurisdictions) access if they agree to contribute funds and share real-time data through a cooperative agreement.[153] It is part of the CDC's National Syndromic Surveillance Program, built in response to a Congressional mandate in the Bioterrorism Preparedness and Response Act of 2002, and later adapted in 2010 to fit broader situational awareness needs of stakeholders.[154]

BioSense aims to provide public health partners with a technology platform to collect and analyze large amounts of health data in a timely manner so that local, state, and federal officials may monitor, detect, and respond to outbreaks and harmful effects from exposure to hazardous conditions.[155] The government distributes funding to public health partners; in 2012 this funding totaled around $7 million, awarded to the 35 participating health departments.[156] A group of non-governmental organizations runs the system, but the CDC (with input from stakeholders) organized and adapted it for broader use. Users include the CDC, state and local health departments, and other public health partners.

The BioSense 2.0 environment,[157] funded by the CDC, is hosted by the Association of State and Territorial Health Officials (ASTHO). Stakeholder feedback is obtained from the ASTHO in coordination with CSTE, the National Association of County and City Health Officials (NACCHO), and the International Society for Disease Surveillance (ISDS). Other federal agencies including the Department of Defense and

[153] *BioSense 2.0*, CDC, http://www.cdc.gov/nssp/biosense/biosense20.html (last visited Aug. 12, 2015).

[154] *BioSense Background*, CDC, http://www.cdc.gov/nssp/biosense/background.html (last visited Aug. 12, 2015).

[155] *BioSense: Meaningful Use*, CDC, http://www.cdc.gov/nssp/biosense/meaningfuluse.html (last visited Aug. 1, 2015).

[156] *BioSense: Cooperative Agreement*, CDC, http://www.cdc.gov/nssp/biosense/cooperativeagreement.html (last visited Aug. 12, 2015).

[157] BioSense 2.0 refers to the latest version of the platform.

Department of Veteran Affairs have assisted in development and integration of the system with existing data systems.[158]

Not all information sharing activities need to be solely funded and administered by the U.S. government. The design of BioSense incentivizes information exchange by making sharing a requirement of participation, and delegating administrative and organizational responsibilities.

V. RECOMMENDATIONS FOR APPLYING INFORMATION SHARING LAWS AND POLICIES TO CYBERSECURITY

We have identified a set of four principles and three information sharing and access models in the public health field that advance public health goals while mitigating the harm to other individual and collective values. Using the derived principles and access methods, we provide a set of recommendations to guide cybersecurity information sharing. These mechanisms and practices facilitate data access for public cybersecurity activities while balancing the privacy, freedom of expression, innovation, and competitiveness of individuals and organizations.

A. CLARIFY THE PUBLIC GOALS OF CYBERSECURITY AND THE ROLE OF INFORMATION SHARING IN ADVANCING THEM

The lack of clarity about overarching goals stymies cybersecurity policy generally, and information sharing specifically. Policy makers should adopt the Doctrine of Public Cybersecurity to ensure that information sharing and other initiatives aid in the production of more secure systems and behaviors, and enable management and response of ongoing vulnerabilities. Assuring that our technical infrastructure is able to adequately secure the activities and data we entrust to it is a pressing national priority. Clarifying the aims of national policy would assure that information sharing and other activities are considered for their capacity to advance these dual goals.

B. CLARIFY CONNECTIONS BETWEEN DATA SHARING PROPOSALS AND PUBLIC GOALS

When advocating information sharing or implementing federal collection, the nexus between the specific information to be shared or collected, its intended use, and relationship to advancing public

[158] *BioSense: The Community*, CDC, http://www.cdc.gov/nssp/biosense/community.html (last visited Aug. 12, 2015).

cybersecurity goals should be clear to contributors and the public. Particularly for data systematically collected or reported through a surveillance system, it is important to make the purpose of collection clear and establish that it will not be used against data subjects for law enforcement or other adverse purposes unrelated to cybersecurity. Uncertainty of end use will negatively impact reporting compliance.

C. COORDINATE ACTIVITIES USING EXPERT COMMUNITIES

Cybersecurity information needs, including information sharing, require expert guidance and coordination. Public health data surveillance is conducted to advance specific goals under the broad umbrella of prevention, response, and management. While it relies upon both state and federal law and public and private sector actors, the federal government coordinates it. The federal government, with input and feedback from public health partners, facilitates agreement on diseases and problems to target, data to collect and share, controls to protect privacy and other values, and the technical and legal mechanisms to implement these policy decisions. The balanced roles between a wide range of stakeholders, and federal partners, offer a model for public cybersecurity information sharing activities.

While the federal government plays the central role in the public health arena, it is unclear whether that is the appropriate approach for cybersecurity given the distribution of expertise and data. Regardless, the federal government can and should play a role in coordinating data and technical standards. Doing so will promote the overall utility and efficiency of information to achieve public cybersecurity goals, and will ensure that privacy and other interests raised by data sharing are thoroughly and systematically addressed. There is a need for coordination and agreement on standards, what data to report, determination of changing data needs to advance public cybersecurity goals, and management on how to distribute the financial burden of these systems among stakeholders. The success of information sharing relies on input from experts and coordination to reflect differing cybersecurity needs.

Several factors complicate the need for coordination. First, cybersecurity lacks uniform agencies equivalent to health departments at the state level. States have taken different approaches to cybersecurity and distributed responsibilities to different state actors. More importantly, cybersecurity incidents lack clear geographic distinctions, and much useful data is in private, not public, institutions. These factors complicate coordination, sharing, and other information governance responsibilities.

Within the public health context, laws regarding information collection and sharing initially developed on a state-by-state basis, with limited federal coordination. It was difficult at the national level to find coherence among these ad hoc laws. Eventually the federal government took on a stronger coordinating role. Finding enough coherence among these ad hoc laws to implement national information sharing and open data practices took many years.

Aspects of the cybersecurity landscape present additional complications beyond those faced in public health. Advanced coordination, therefore, is particularly important. Expertise is spread across many stakeholders: those who run infrastructure, those who develop tools to defend it, and those who represent the interests of system users. To date, a subset of these experts have driven policy deliberations. In particular, civil society organizations, representing the interests of users and supporting values such as privacy, have been relegated to a largely reactive role. Ensuring that all stakeholders with expertise are able to participate in defining the cybersecurity information sharing ecosystem is key to achieving widespread public support for information sharing in this context. Such inclusion was essential to achieving such public support for information sharing in the public health arena.

D. WHERE POSSIBLE, FOSTER VOLUNTARY INFORMATION SHARING COLLABORATIONS

The majority of reported data and public health surveillance systems within this Article were a result of voluntary state and private industry collaborations with the federal government. Currently, many cybersecurity data are voluntarily shared. However, both the scope of, and participation in, these systems is limited. Cybersecurity policy could build out mechanisms illustrated in public health, like the formation of CSTE-like committees of stakeholders, to foster greater community input and collaboration in these systems. Existing information sharing organizations, like ISACs, could serve as foundations for expanding the role and coordinating capacity of stakeholders. Other organizational strategies, such as allowing non-governmental organizations (like those involved in the creation and maintenance of BioSense 2.0) to store and manage data systems may also encourage information sharing. If coupled with the sorts of privacy-sensitive approaches discussed below (particularly law enforcement actions against individuals for non-cybersecurity issues), this can also reduce concerns about the use of shared information for secondary purposes.

E. EMPHASIZE DATA MINIMIZATION, DECENTRALIZATION, AND EARLY DE-IDENTIFICATION

Wherever possible, personally identifiable information should not be collected or shared to support cybersecurity activities. Federal public health reports note that the balance between the need for data sharing and data protection influences how willingly data providers contribute or withhold data.[159] Where personally identifiable data are necessary, they should remain only at the source of collection or intervention. Policies and mechanisms that protect privacy will increase the willingness of entities to share information, and increase the willingness of all stakeholders to consider the potential public cybersecurity benefits of information sharing strategies.

F. PROVIDE ADDITIONAL PRIVACY PROTECTIONS THROUGH NATIONAL INFORMATION SHARING LAWS

The public health system encourages participation by reducing the possibility that information collected for public health purposes will be used to the detriment of individuals. Providing similar protections would build greater acceptance for information sharing. Cybersecurity policies have generally lacked provisions tightly limiting the use of shared information. Their absence has been a major source of objection for civil society stakeholders. Provisions should limit the use of shared information to advancing the public cybersecurity goals of producing better systems and behaviors, manage insecurity, and specifically prohibit the use of information for law enforcement activities that do not directly advance these goals. As in public health, meaningful penalties for violations should accompany these prohibitions and limitations on use. In addition, it would be beneficial to provide protections similar to those afforded by Certificates of Confidentiality, which protect researchers who use public health data from being compelled to release it for legal proceedings. As with public health, sound public cybersecurity policy depends upon ongoing evaluation of the utility of interventions. This research may also involve personally identifiable information, and it too should be protected against disclosure.

[159] CDC-ATSDR DATA RELEASE GUIDELINES AND PROCEDURES, *supra* note 92, at 5.

G. MAKE AS MUCH CYBERSECURITY DATA AS POSSIBLE OPEN AND ACCESSIBLE FOR PUBLIC USE

As in the field of public health, as much data as possible should be made open and accessible for public use in order to promote public cybersecurity goals. The federal government consolidates and curates public health data and makes it accessible to many stakeholders—from citizen to corporation—through a variety of access and sharing mechanisms.

Data that cannot be made open should be as accessible as possible through limited data access mechanisms and special use agreements. As illustrated in the previous sections, public health takes advantage of several data access modes (public access, access mediated with some restrictions, or no access) to make information accessible for approved purposes. Though data are made as open as possible for public use, great consideration is given to individual privacy and the tradeoffs between accessibility and confidentiality. For public health data offered with some restrictions, the use of RDCs and the ability to run code on sensitive datasets remotely both protect data without inhibiting potential uses.

Data need not be held by the federal government in order to facilitate public access—even for data that requires use and availability restrictions. Data about networked interactions and the state of machines and devices, held and shared only across the private sector, can aid cybersecurity goals. While no single entity has a total view of the data, many have extensive information and insight into the security posture of pieces of the system. It may be far easier, more efficient, and less controversial to bring analysis tools to the data than to bring the data to the government for analysis. While government efforts to advance public cybersecurity goals undoubtedly would benefit from more data, the extent to which the federal government is the appropriate entity to collect it is decidedly unclear. As in public health, multiple models for information collection and access can help balance public cybersecurity goals and other values.

H. CYBERSECURITY SHARING PRACTICES SHOULD EMPHASIZE ETHICAL PUBLIC CYBERSECURITY RESEARCH

Research is essential to many public health goals and is equally important for public cybersecurity. Research evaluates the effectiveness and efficiency of programs, and allows for the formulation of recommendations for improvement. Both preventative and response objectives rely heavily on data and analysis from ongoing research activities. The 1979 Belmont Report guides human subject research activities within the United States, including public health research as it pertains to interventions or interviews.[160] Built off the canonical Belmont Report, the 2012 Menlo Report[161] establishes an ethical framework for computer and information security research by introducing four core ethical principles, as well as methods to operationalize those principles in the research domain. The core ethical principles include respect for persons, beneficence, justice, and respect for law and the public interest.

Public cybersecurity's primary orientation is focused on society as a whole rather than upon any one individual. But it is vital that data collection and research activities respect individual persons or groups of people who are impacted by data collection, data release, and generalized research findings, or who might ultimately be subjected to containment measures. When promoting public cybersecurity goals, the rights and autonomy of individuals must constantly be factors. Implementing public cybersecurity activities will require tradeoffs between public benefit and individual rights and interests (Table 2). There should also be consideration of how the distribution of the burdens and risks of participation align with the distribution of benefits from public cybersecurity research. For instance, it would not be in the interests of justice to place the administrative burden of information reporting or the loss of privacy disproportionately on one segment of the population unless they were disproportionately to benefit. The selection of subjects within research should be fair, and the burdens should be allocated as equitably as possible so that the risks and benefits are shared among impacted populations. It is imperative that all activities—including information sharing activities—attend to these tensions and tradeoffs, and involve systematic reevaluation of the risks, benefits and burdens as threats evolve.

Table 2: Tradeoffs Between Data Collection and Surveillance for Response Orientation Public Good Activities

Public Benefit Derived from Data Use	Public Good Activity	Public Interests/Rights

[160] NAT'L COMM'N FOR THE PROTECTION OF HUMAN SUBJECTS OF BIOMEDICAL & BEHAVIORAL RESEARCH, THE BELMONT REPORT: ETHICAL PRINCIPLES AND GUIDELINES FOR THE PROTECTION OF HUMAN SUBJECTS RESEARCH (1979), http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html.

[161] THE MENLO REPORT: ETHICAL PRINCIPLES GUIDING INFORMATION AND COMMUNICATION TECHNOLOGY RESEARCH (2012), http://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803.pdf.

• Manage insecurity from known threats through systematic, organized monitoring • Alerts for unidentified anomalies and new/emerging threats • Immediate contacting of stakeholders affected by detected incident • Ability to trigger other public good activities	• Detection	• Personal autonomy • Individual privacy • Freedom of action • Business interests
• Distinguish between new or recurring threats • Coordinate experts to classify threat or incident • Determine risk and response level • Public announcements about threat/incident	• Identification	• Personal autonomy • Individual privacy • Business interests
• Enable localized and individual action in response to incident • Empower collective action in response to threat • Inform response at many levels to quarantine, patch, or screen for malicious activity • Implement improved preventative techniques to prevent spread to other vulnerable machines and systems	• Containment	• Personal autonomy • Individual privacy • Freedom of action • Business interests • Freedom to innovate
• Appropriately allocate benefits and services to assist recovery • Treat affected and vulnerable populations with patch or design change	• Treatment	• Personal autonomy • Freedom of action • Freedom to innovate

VI. CONCLUSION

Information sharing is a means to an end. Its utility must be assessed based on its capacity to support public cybersecurity goals. Orienting cybersecurity policy toward prevention by a reduction in vulnerabilities and response by managing insecurity, would advance the security of our networks and data. Meeting these objectives will depend on coordinated activities enabled by information. Within public health, information sharing has advanced specific goals and outcomes, in addition to fueling research that has directly and indirectly benefited public health. There are many options for sharing data with different stakeholders and with differing degrees of openness. Laws and institutional policies and practices developed over time in public health provide a rich model that can inform cybersecurity information sharing. This model reflects the need to strike balances between competing public values and the interests of the individual and the collective. The organizational and governance models, policies that address competing values such as privacy, and access mechanisms found in public health provide useful guidance for the development of sound public cybersecurity policy.

VII. APPENDIX

Public health principles rest heavily on the belief that people are interdependent, which underscores the essence and importance of considering the community. We believe this is also important in the case of cybersecurity, both because networks and systems connect people and data about people, and because there are many communities of practice surrounding cybersecurity.

Table 3: Core Public Health Ethical Principles Applied to Cybersecurity

Principles of the Ethical Practice of Public Health	Application to Practice of Public Cybersecurity
1) Public health should address principally the fundamental causes of disease and requirements for health, aiming to prevent adverse health outcomes.	Public cybersecurity should address systemic design weaknesses and underlying behavioral causes through the preventative orientation to prevent adverse security outcomes.
2) Public health should achieve community health in a way that respects the rights of individuals in the community.	Public cybersecurity should achieve community health in a way that respects the rights of individuals in the community..
3) Public health policies, programs, and priorities should be developed and evaluated through processes that ensure an opportunity for input from community members.	Public cybersecurity policies, programs, and priorities should be developed and evaluated through processes that ensure an opportunity for input from community members.

Principles of the Ethical Practice of Public Health	Application to Practice of Public Cybersecurity
4) Public health should advocate and work for the empowerment of disenfranchised community members, aiming to ensure that the basic resources and conditions necessary for health are accessible to all.	Public cybersecurity should advocate and work for the empowerment of disenfranchised community members (all individual users, all private companies and organizations regardless of size)
5) Public health should seek the information needed to implement effective policies and programs that protect and promote health.	Public cybersecurity should seek the information needed to implement effective policies and programs that protect and promote healthy networks, systems, infrastructure, and use of Internet-based communication.
6) Public health institutions should provide communities with the information they have that is needed for decisions on policies or programs and should obtain the community's consent for their implementation.	Public cybersecurity institutions should provide communities and stakeholders with the information they have that is needed for decisions on policies or programs and should obtain the community and stakeholder's consent for their implementation.
7) Public health institutions should act in a timely manner on the information they have within the resources and the mandate given to them by the public.	Public cybersecurity institutions should act in a timely manner on the information they have within the resources and the mandate given to them by the public..
8) Public health programs and policies should incorporate a variety of approaches that anticipate and respect diverse values, beliefs, and cultures in the community.	Public cybersecurity programs and policies should incorporate a variety of approaches that anticipate and respect diverse values, beliefs, and cultures in the community.
9) Public health programs and policies should be implemented in a manner that most enhances the physical and social environment.	Public cybersecurity programs and policies should be implemented in a manner that most enhances the physical and social environment.
10) Public health institutions should protect the confidentiality of information that can bring harm to an individual or community if made public. Exceptions must be justified on the basis of the high likelihood of significant harm to the individual or others.	Public cybersecurity institutions should protect the confidentiality of information that can bring harm to an individual or community if made public. Exceptions must be justified on the basis of the high likelihood of significant harm to the individual or others.
11) Public health institutions should ensure the professional competence of their employees.	Public cybersecurity institutions should ensure the professional competence of their employees.
12) Public health institutions and their employees should engage in collaborations and affiliations in ways that build the public's trust and the institution's effectiveness.	Public cybersecurity institutions and their employees should engage in collaborations and affiliations in ways that build the public's trust and the institution's effectiveness.

In Table 3, we adapted the key principles within the code of ethics developed by the Public Health Leadership Society to illustrate how they map directly onto the distinctive characteristics found in the doctrine of public cybersecurity.[162] These principles provide guidance during all public good activities and are offered as a way of balancing tensions between collective benefit and individual values, as well as on how to engage various interests of communities and stakeholders. It should be noted that principles 5 through 7 relate specifically to the collection of information, imperative to act upon information, and responsibility to present information to the public. We believe these values support our recommendations on applying public health information sharing mechanisms in the public cybersecurity sphere.

[162] PUBLIC HEALTH LEADERSHIP SOCIETY, PRINCIPLES OF THE ETHICAL PRACTICE OF PUBLIC HEALTH VERSION 2.2 (2002), http://phls.org/CMSuploads/Principles-of-the-Ethical-Practice-of-PH-Version-2.2-68496.pdf.