Nebraska Law Review

Volume 96 | Issue 2 Article 7

2017

What's Next for E-Government? Innovations in E-Government Through a Cybersecurity Lens

Emefa Agawu
New America, agawu@newamerica.org

Emefa Agawu*

What's Next for E-Government? Innovations in E-Government Through a Cybersecurity Lens

TABLE OF CONTENTS

I. INTRODUCTION

Much has been made of the staggering impact of the rapidly digitizing world. Technological innovations often outpace our ability to fully understand how they affect us. However, rather than presenting entirely new paradigms, we often use some form of digital technology in pursuit of a relatively unchanged end goal. One might employ a digital platform to have food delivered or to decide what to eat, use a

* Emefa Addo Agawu is a Program Associate in New America's Cybersecurity Initiative, where she leads work on state and local cybersecurity.

mobile application to measure and optimize sleep habits, or rely on digital services to facilitate social interactions, but the essential end goals of eating, sleeping, and socializing are not unrecognizable from their earlier forms.

This pattern is often the case with e-government and service provision. State and local government entities generally perform their duties in resource-scarce environments—low on capital, low on personnel, and low on time. Highlighting the revenue shortages facing states, the Center on Budget and Policy Priorities reports that in 2017, "25 states are facing or have addressed revenue shortfalls" and "[m]ore states expect mid-year revenue shortfalls than in any year since 2010."[1] In such a context, it is unsurprising that governments, often in an ad hoc manner, rely increasingly on digital processes to assist in governing functions.[2] Not unlike commercial applications, government entities are often digitizing ancillary systems and procedures for efficiency or optimization, while leaving the essential governing function unchanged. For an obvious example, today one might register to vote using an online system rather than mailing or physically returning a paper form.[3]

Champions of technology adoption by governments for service provision point to the many benefits for constituents. It is a thin line between claims that are exaggerated and those that are merely enthusiastic. Seifert and Peterson argue that e-government has the potential to transform citizen access and participation,[4] whereas Norris and Reddick critically present a large, overenthusiastic literature arguing for e-government's ability to enhance access, quality, transparency, and efficiency in government.[5] Yet, there is evidence to support the claims of the optimists. When it comes to voter registration, a 2015 Brennan Center report found that electronic and online registration increased voter-roll accuracy, saved money, and boosted registra-

1. ELIZABETH MCNICHOL & SAMANTHA WAXMAN, CTR. ON BUDGET & POLICY PRIORITIES, MANY STATES FACE REVENUE SHORTFALLS: STATES CAN TAKE STEPS TO STRENGTHEN THEIR TAX SYSTEMS AND RESERVES 1 (2017), http://www.cbpp.org/sites/default/files/atoms/files/3-30-17sfp.pdf [https://perma.unl.edu/8YQS-5AT9].

2. *See* TECH TRENDS 2017: THE KINETIC ENTERPRISE (Bill Briggs ed., 2016), https://dupress.deloitte.com/content/dam/dup-us-en/articles/3468_TechTrends2017/DUP_TechTrends2017.pdf [https://perma.unl.edu/E5NB-XMDF].

3. *Online Voter Registration*, NAT'L CONF. ST. LEGISLATURES (Jan. 31, 2017), http://www.ncsl.org/research/elections-and-campaigns/electronic-or-online-voter-registration.aspx [https://perma.unl.edu/9MM9-2ACL].

4. Jeffrey W. Seifert & R. Eric Petersen, *The Promise of All Things E? Expectations and Challenges of Emergent Electronic Government*, 1 PERSP. ON GLOBAL DEV. & TECH. 193 (2002).

5. Donald F. Norris & Christopher G. Reddick, *Local E-Government in the United States: Transformation or Incremental Change?*, 73 PUB. ADMIN. REV. 165, 166 (2012).

tion rates.[6] However, with online voter registration, as with other e-government innovations, while the end goal is largely the same, the security considerations are not.[7] Furthermore, it is not always the case that governments use technology to digitize existing services. In some instances, they create—whether intentionally or not—new governing functions.

The pace and particularities of technology in state and local government can be difficult to follow, not least because of the sheer number of units to keep up with. The 2012 census counted 89,004 local governments in the United States.[8] Dawes outlines the major technology, policy, and implementation developments associated with e-governance, characterizing the computing innovations within government from pre-1990 through post-2000 by tracing the evolution of desktop computing, local networks, wireless network and mobile computing, data mining, Web 2.0 tools, and more.[9] A number of sites, magazines, and journals chronicle technology adoption in various levels of government—Government Technology Magazine and State Tech Magazine, among others. One only has to glance at the headlines to get a sense of the enormous scope of the disparate ways in which the government uses technology for its aims, ranging from automating snow plowing to creating online town halls.

The range of accompanying risks is as broad as the types of technology being adopted. Put together, technology adoption and its associated, expanding-threat landscape can seem overwhelming. How can we understand the dizzying and diverse array of e-government innovations, and how can we make sense of the cybersecurity concerns they raise?

This Article attempts to answer those questions with two contributions. First, this Article offers a framework through which to understand distinct trends in e-government. Second, the Article applies the classic CIA information-security triad to these trends, suggesting that policy makers and future analysis would be well served in adopting a similar approach. The Article ends with consideration of two relevant

6. HOLLY MALUK, MYRNA PEREZ & LUCY ZHOU, BRENNAN CTR. FOR JUSTICE, VOTER REGISTRATION IN A DIGITAL AGE: 2015 UPDATE 3–8 (2015), https://www.brennancenter.org/sites/default/files/publications/Voter_Registration_Digital_Age_2015.pdf [https://perma.unl.edu/D8KQ-LLKM].

7. *See* Open Letter from J. Alex Halderman et al. to Maryland State Board of Elections (Sept. 25, 2012), https://www.verifiedvoting.org/wp-content/uploads/2013/04/maryland-online-voting-concerns.pdf [https://perma.unl.edu/CM5H-EJ55].

8. Press Release, U.S. Census Bureau, Census Bureau Reports There Are 89,004 Local Governments in the United States (Aug. 30, 2012), https://www.census.gov/newsroom/releases/archives/governments/cb12-161.html [https://perma.unl.edu/Q2WW-ZE4R].

9. Sharon S. Dawes, *The Evolution and Continuing Challenges of E-Governance: The Quest for High-Performance Administration*, 68 PUB. ADMIN. REV. S86, S91 (2008).

e-government initiatives—Open Data Initiative in New Jersey and the Mayor's Office of New Urban Mechanics in Boston.

II. WHAT IS E-GOVERNMENT?

There are many terms used to refer vaguely to the use of technology within government, including, but not limited to: digital government, e-democracy, e-government, and e-governance. In addition to the overlapping definitions in the academic literature, there are government actors in the field who may employ altogether different rhetoric to describe their activities. As Bannister and Connolly point out, "e-government" and "e-governance" are difficult to define, in no small part, because "government" and "governance" are difficult to define.[10] While some use the terms e-government and e-governance interchangeably, many authors find e-governance to be a more encompassing category than e-government.[11] This Article is informed by West's useful definition of e-government as "the delivery of [government] information and services online through the Internet or other digital means."[12] Recognizing how quickly innovations occur in this space, this definition will suffice.

There are four commonly referenced directions of activity in e-government, categorized by the constituency that interacts with the governmental body (G). They are government-to-citizen (G2C), government-to-business (G2B), government-to-government (G2G), and government-to-employee (G2E).[13] While the use of technology affects each of these interactions, this Article is only concerned with the first category of activity: government-to-citizen interaction.[14]

In considering governmental service delivery, I propose three trends that capture the current state of G2C activity: (1) increasing access to information, which is the use of digital platforms or services to facilitate citizen access to relevant content; (2) digitizing the service loop, which is the process of digitizing some element of the govern-

10. *See* Frank Bannister & Regina Connolly, *Defining E-Governance*, 8 E-SERV. J. 3 (2012).
11. *See id.* (discussing the difference between e-government and e-governance).
12. Darrell M. West, *Assessing E-Government: The Internet, Democracy, and Service Delivery by State and Federal Governments*, NAT'L SCI. DIGITAL LIBR. (Sept. 2000), http://nsdl.oercommons.org/courses/assessing-e-government-the-internet-democracy-and-service-delivery-by-state-and-federal-governments/view [https://perma.unl.edu/92MJ-PHZL].
13. For more on the basics of e-government, see Mohammed Alshehri & Steve Drew, *E-Government Fundamentals*, *in* PROCEEDINGS OF THE IADIS INTERNATIONAL CONFERENCE ICT, SOCIETY AND HUMAN BEINGS 2010, at 35 (2010), https://research-repository.griffith.edu.au/bitstream/handle/10072/37709/67525_1.pdf [https://perma.unl.edu/5XMV-K9KP].
14. "Citizen," as used herein, is not intended to make comment about legal status but rather to mean constituent, resident, community member, or user of government services.

ment service while leaving the essential function unchanged; and (3) expansion or creation of new governance function, which is the use of technology to expand or create a government service that cannot readily be said to have a non-digital parallel. Part III introduces each of these trends, offering examples to show the range of activity.

III. TRENDS IN E-GOVERNMENT INNOVATION

When it comes to government service delivery, I have identified three categories of activity. While it is tempting to present these categories in terms of stages, implying maturity or path-directional movement, this is not necessarily the case, and the ad hoc nature in which decisions about integrating technology into various government functions is already upsetting and is sure to continue to upset any narrow theoretical pathways. Any one of the objectives detailed below may be desirable in its own right, and a government actor can reasonably aim to achieve one without seriously pursuing one or both of the other objectives.

A. Increasing Access to Content

Increasing access to relevant content is perhaps the most obvious and intuitive objective when considering how governments interact with citizens. This goal is associated with increasingly popular themes, such as open data. The motivations behind open-data initiatives range from transparency and accountability to equipping social scientists with richer datasets to inform their work. President Obama's 2013 Executive Order made open and machine-readable data the new default for government information,[15] but the federal government is neither the only nor the first government entity to embrace the concept of open data.

The Sunlight Foundation, supported by Bloomberg Philanthropies' What Works Cities project, developed opendatapolicies.org, which provides a list of open-data policies for various jurisdictions around the country. As of February 2017, the diverse list includes places like Boston, Massachusetts; Cook County, Illinois; New Jersey; and Wichita, Kansas.[16]

However, the access-to-content objective is broader than just open data, which itself is not always clearly defined. In his 2005 book, *Digital Government: Technology and Public Sector Performance*, Darren West describes four stages of e-government. He calls the first the "billboard stage," in which "officials treat government websites much in

15. *See* Archive of *Open Government Initiative*, OBAMA WHITE HOUSE, obamawhitehouse.archives.gov/open [https://perma.unl.edu/M7FN-UK92].

16. *See* OPEN DATA POL'Y COLLECTION, http://www.opendatapolicies.org [https://perma.unl.edu/8JCN-B4NJ].

the way highway billboards are used, that is, static mechanisms to display information. They post reports and publications, and offer databases for viewing by visitors."[17] Today this could include posting alerts on government websites and live streaming or archiving community meetings or community working groups. This is often achieved by using a nongovernmental platform, such as YouTube.[18]

However, there is a broader range of relevant content a government might wish to provide to its citizens. Governments are increasingly making use of social media to communicate timely content to citizens. A 2014 working paper overviews the ways that "[g]overnment institutions are slowly becoming more represented and active on social media," pointing out that "the main executive institutions in 26 out of 34 OECD member countries operate a Twitter account; and they maintain a Facebook page in 21 out of 34 countries. Many ministries and specialised agencies operate on social media; as do institutions at regional and local levels of government."[19]

In the United States, governments also use social media below the federal level. A 2012 survey from the National Association of State Chief Information Officers (NASCIO) found that "100% of respondents reported that their states use social media in some manner. 83% use Facebook moderately or widely, while 81% use Twitter moderately or widely and 83% use YouTube moderately or widely."[20] The same survey found that "[n]o states are prohibiting the use of social media by their agencies."[21] Government use of social media is rightly the subject of much conversation both in and out of academia. From its utility in crisis communication and emergency management to building trust in government, some embrace the benefits of government use of social media, while others remain wary.

More recently, the first-time use of a law enforcement emergency alert in New York on the morning of September 19, 2016, raised the prospect of future and expanded use. After an explosion in Manhattan, city officials from the NYPD, the FBI, and the Office of Emer-

17. *See* DARRELL M. WEST, DIGITAL GOVERNMENT: TECHNOLOGY AND PUBLIC SECTOR PERFORMANCE 9 (2005).

18. A YouTube search for "city council meeting" will return literally millions of results, though more than a few are parodies.

19. Arthur Mickoleit, *Social Media Use by Governments: A Policy Primer to Discuss Trends, Identify Policy Opportunities and Guide Decision Makers* 2 (OECD Working Papers on Public Governance, Paper No. 26, 2014), http://www.oecd-ilibrary.org/docserver/download/5jxrcmghmk0s-en.pdf?expires=1503272782&id=id&accname=guest&checksum=CFF33A48D5D6CA28F6AD80C2A4C8929C [https://perma.unl.edu/H82B-69RQ].

20. NAT'L ASS'N OF STATE CHIEF INFO. OFFICERS, EXAMINING STATE SOCIAL MEDIA POLICIES: CLOSING THE GAPS 1 (2013), https://www.nascio.org/Portals/0/Publications/Documents/NASCIO_2013SocialMediaIssueBrief.pdf [https://perma.unl.edu/L55G-8P6C].

21. *Id.*

gency Management activated a message system that sent a notification to smartphone owners in the area, directing them to call 9-1-1 if they saw the man wanted in connection to the incident.[22] The Federal Communications Commission website explains that "[p]re-authorized national, state or local government authorities may send alerts regarding public safety emergencies, such as evacuation orders or shelter-in-place orders due to severe weather, a terrorist threat or chemical spill."[23] In emergency situations, we may see direct alerts being used more frequently in the future, including from state and local forces.

B. Digitize Service Loop

Another objective that government officials often have when integrating technology is to digitize some or all of a governing function in a way that does not fundamentally change that function. In its broadest form, imagine a service-provision loop: information or materials are sent out from government and received by the citizen, acted upon, and returned in some form to the government. Digitizing the service loop refers to digitizing some, or all, of that process while leaving the core function unchanged. This often takes the form of electronic record keeping and submissions. This digitization, while leaving essential functions unchanged, can have dramatic effects by increasing efficiency and speed in a way that improves the accessibility of a service.[24] Indeed, these effects are often drivers of technology adoption.

Like open data and other measures to increase access to content, digitizing the service loop has been happening in state and local governments across the country for years. One common process to move online is voter registration. According to the Brennan Center, as of February 3, 2017, at least thirty-five states and the District of Columbia currently or will soon have fully or substantially electronic voter registration at DMVs, and twenty-eight states and the District of Columbia currently or will soon offer online voter registration.[25]

22. Seth Fiegerman, *The Story Behind the Smartphone Terror Alert in NYC*, CNN (Sept. 19, 2016), http://money.cnn.com/2016/09/19/technology/chelsea-explosion-emergency-alert/index.html [https://perma.unl.edu/TC6H-R5ES].

23. *Id.*

24. Consider, for example, the promise of automatic voter registration to boost voter registration and turnout. *See generally* TOMAS LOPEZ ET AL., BRENNAN CTR. FOR JUSTICE, THE CASE FOR AUTOMATIC VOTER REGISTRATION (2016), https://www.mcf.org/sites/default/files/files/news/Case_for_Automatic_Voter_Registration.pdf [https://perma.unl.edu/7329-75QB].

25. *Automatic Voter Registration and Modernization in the States,* BRENNAN CTR. FOR JUST. (Feb. 3, 2017), https://www.brennancenter.org/analysis/voter-registration-modernization-states [https://perma.unl.edu/YTS9-NMRL].

Digitizing processes is not reserved to any one kind of department. Examples range from renewing licenses and paying speeding tickets online to filing federal or state taxes online. In many cases, there remains a paper version of the process. Elsewhere, departments are attempting to do away with paper processes altogether. In addition to asking how much of the service loop is *possible* to do online, it is also relevant to ask how much of the service *must* be done online. There are three options. The service can be done: (1) entirely online, (2) partially online and partially offline, or (3) entirely offline. For instance, in some states, one can choose to register to vote entirely online, entirely offline, or partially online and offline.[26] However, some government departments are pushing for entirely paperless processes for reasons of efficiency or environmental consciousness.

C. Expand or Create New Government Functions

A third objective governments may have when integrating technology into service delivery is to expand or create new government functions. This occurs when a government uses the integration of technology to create a new function that does not have a nondigital parallel. This category is the murkiest, but it is also one that many governments are extremely enthusiastic about as it is often seen as a way of restoring faith in government or democracy.[27] In some instances, governments use technology to take on roles they did not previously have, either entirely on their own or in conjunction with a third party.

Upon winning the Bloomberg Philanthropies' 2013 Mayors Challenge, the town of Providence, Rhode Island, received five million dollars to develop a program called Providence Talks. The purpose of the voluntary early-intervention program is to:

> do something never before attempted at the municipal level: to intervene at a critically early age, from birth to age three, to close the "30 million word gap" at a city-wide scale and ensure that every child in Providence enters a kindergarten classroom ready to achieve at extraordinary levels.[28]

The program served 170 families in its pilot phase, distributing "small, wearable recording devices [that] record up to sixteen hours of what a child hears in the course of the day. Software automatically analyzes the recording and counts the number of words, interactions . . . and media exposure. The recording, which is never listened

26. PEW CHARITABLE TRS., ONLINE VOTER REGISTRATION: TRENDS IN DEVELOPMENT AND IMPLEMENTATION 4 (2015), http://www.pewtrusts.org/~/media/assets/2015/05/ovr_2015_brief.pdf [https://perma.unl.edu/8FH8-HP3Q].

27. *Civic Technology—1—Saving Democracy?*, PARIS INNOVATION REV. (Mar. 8, 2017), http://parisinnovationreview.com/2017/03/08/civic-technology-1-saving-democracy [https://perma.unl.edu/9ZNG-C9VQ].

28. *See* PROVIDENCE TALKS, http://www.providencetalks.org [https://perma.unl.edu/LXV8-5RKX].

to, is then securely deleted."[29] This information is then presented to families to help parents adjust and create an environment conducive to boosting vocabulary. This innovation is an example of a local government using technology to support its citizens in new ways.

This sort of innovation is not confined to the United States. In anticipation of the care needs of a growing elderly population, the city of Barcelona is launching a digital platform that "brings together and coordinates the support of friends, family members, neighbors, and professional care givers around at-risk seniors."[30] The program, an initiative of the Barcelona City Council's Quality of Life, Equality and Sports Department, began in 2016 in two neighborhoods and is expanding operations in 2017.[31] These two examples are offered not to weigh in on their wisdom from a cybersecurity perspective but rather to offer two very different examples of the sort of innovation and programs local governments are pursuing.

Another relevant area of innovation is in so-called civic technology. The burgeoning field of civic technology overlaps with the discussion here. A 2013 report from the Knight Foundation identifies eleven civic-technology innovation clusters and files them under either Open Government (including data access, data transparency, and resident feedback) or Community Action (including civic crowdfunding and community organizing).[32] The Community Action category is not relevant to this analysis because the government is not an actor. It is not clear that the entirety of the former category (Open Government) is of interest here, but the overlap is more obvious.

The literature on civic technology is sparse, largely due to its novelty and variability. In a recent exploratory paper, Gilman sets out to begin a rigorous study into the field. Gilman defines civic technology as "*technology that is explicitly leveraged to increase and deepen demo-*

29. PROVIDENCE TALKS, PILOT FINDINGS AND NEXT STEPS 3 (2015), http://www.providencetalks.org/wp-content/uploads/2015/10/Providence-Talks-Pilot-Findings-Next-Steps.pdf [https://perma.unl.edu/E7NB-SSSM].

30. *See Vincles BCN: Collaborative Care Networks for Better Aging*, BLOOMBERG PHILANTHROPIES, http://mayorschallenge.bloomberg.org/ideas/collaborative-care-networks-for-better-aging [https://perma.unl.edu/PC22-ZHJ5].

31. *Id.*; *see* JEFF VINING, GARTNER, HOW LOCAL GOVERNMENT CIOS CAN IMPROVE MOBILE APP STRATEGIES (2015), http://nascio.org/events/sponsors/vrc/How%20Local%20Government%20CIOs%20Can%20Improve%20Mobile%20App%20Strategies.pdf [https://perma.unl.edu/5RG5-RCDV].

32. *See* KNIGHT FOUND., DIGITAL CITIZENSHIP: EXPLORING THE FIELD OF TECH FOR ENGAGEMENT (2012), https://www.knightfoundation.org/media/uploads/media_pdfs/Digital-Citizenship-tech4engage-summit-report.pdf [https://perma.unl.edu/8BD6-KG76]; Knight Found., *The Emergence of Civic Tech: Investments in a Growing Field*, SLIDESHARE (Dec. 3, 2013), http://www.slideshare.net/knightfoundation/knight-civictech [https://perma.unl.edu/BZ9L-TZBB].

cratic participation,"[33] excluding technology that is used solely for modernization or market gain. However, while Gilman is less concerned with who is doing the leveraging (e.g., government or community group), this Article focuses on technology being leveraged by a government actor. Gilman goes on to present three case studies: Chicago's Open Data, Civic Crowdfunding in Rhode Island, and the Mayor's Office of New Urban Mechanics (MONUM) in Boston. Despite our differing focuses, there are overlapping areas of analytical interest. Specifically, we both highlight MONUM. Leaving aside questions of whether it is appropriate for government to take on these functions or what impact this would have on the market or larger policy ecosystem, it is clear that taking on new responsibilities and digital assets presents new cybersecurity questions.

IV. STATE AND LOCAL GOVERNMENTS IN A CHANGING THREAT LANDSCAPE

The use of digital technology brings with it a number of threats from which state and local governments are not immune. For example, ransomware—the worrying trend in which hackers encrypt or otherwise block access to data until a ransom is paid—is increasingly targeted at state and local governments, police departments, and agencies.[34] State-run voter-registration systems were targeted during the 2016 election,[35] with successful breaches of at least two.[36]

There are a number of challenges in obtaining a mature cybersecurity posture in state and local government, structural and otherwise. One major challenge is attracting and retaining cybersecurity talent for state- and local-government jobs. A 2015 NASCIO survey of forty-eight states found that in ninety-two percent of states, salary

33. Hollie Russon Gilman, *Civic Tech for Urban Collaborative Governance*, 50 PS: POL. SCI. & POLS. 744, 745 (2017).

34. *See Malware, Ransomware Twice as Likely to Hit State, Local Networks*, GCN (Dec. 1, 2015), https://gcn.com/articles/2015/12/01/sled-ransomware.aspx [https://perma.unl.edu/T2FT-HY9A] (stating states and localities are twice as likely to get hit); *see also* Kelly Jackson Higgins, *State & Local Government Hit by Malware, Ransomware More than SMBs*, DARK READING (Nov. 30, 2015), http://www.darkreading.com/attacks-breaches/state-and-local-government-hit-by-malware-ransomware-more-than-smbs/d/d-id/1323355 [https://perma.unl.edu/FUY8-N7T2] ("[N]early 70% of state and local government networks triggered malware or ransomware alerts . . . .").

35. Brian Feldman, *The Election Wasn't Hacked—At Least, Not in the Way You Think*, SELECT ALL (Nov. 14, 2016), http://nymag.com/selectall/2016/11/the-election-wasnt-hacked-at-least-not-how-you-think.html [https://perma.unl.edu/SC8K-YPQ3].

36. Wesley Bruer & Evan Perez, *Officials: Hackers Breach Election Systems in Illinois, Arizona*, CNN (Aug. 30, 2016), http://www.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems [https://perma.unl.edu/WL32-YTBF].

and pay-grade structures are a challenge in attracting and keeping employees; eighty-six percent of states have difficulty recruiting people to fill vacant slots; and security is the skill that presents the greatest challenge in attracting and retaining IT employees.[37]

Second, in many instances, digital technology at the state and local levels has been adopted in an ad hoc matter as the need arose, often without centralized oversight. This has led, in many cases, to sprawling systems with duplicative functions and non-integrated assets and networks, all of which can increase cyber risk.[38]

Third, as is commonly observed, to prevent a cyber incident, the network defenders have to be alert to *every* potential cyber attack. To be successful, the attackers only have to be right once. This reality dramatically increases the potential cost of error.[39]

Finally, as service providers, governments often have to update systems and react to incidents while they execute essential functions. Unlike in other sectors, where there may be more flexibility in going offline to address issues, governments often have to deal with cybersecurity matters while continuously providing services.

Decision makers in state and local governments juggle various priorities and often operate in resource-starved environments. Their decision-making calculus around integrating technology into government-to-citizen service provision may be dominated by many concerns, from cost savings to renewing citizen trust in government. The extent to which these actors consider cybersecurity varies drastically.

In some states and localities, there is a patchwork of regulatory guidance for government actors to consider. The National Governor's Association (NGA), in partnership with Day Pitney LLP, released a primer that overviews the diverse federal regulatory environment that states operate in with respect to cybersecurity.[40] The National Institute of Standards and Technology (NIST) Cybersecurity Frame-

37. NAT'L ASS'N OF STATE CHIEF INFO. OFFICERS, STATE IT WORKFORCE: FACING REALITY WITH INNOVATION 3 (2015), https://www.nascio.org/Portals/0/Publications/Documents/NASCIO_StateITWorkforceSurvey2015_WEB.pdf [https://perma.unl.edu/F2PM-WCXN].

38. For more on IT consolidation, see LEADERSHIP FOR A NETWORKED WORLD, THE TRANSFORMATION OF THE STATE OF OHIO COMPUTING CENTER 4–5 (2016), http://das.ohio.gov/Portals/0/DASDivisions/InformationTechnology/IS/Optimization/2016%20NASCA%20Ohio%20Case%20Study.pdf [https://perma.unl.edu/HRY7-8748].

39. This truism is summarized: "As on the internet, attack is easier than defense." For expanded discussion on this and other truisms around cybersecurity, vulnerabilities, and the future, see Bruce Schneier, *Click Here to Kill Everyone,* SELECT ALL (Jan. 27, 2017), http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html [https://perma.unl.edu/93UN-RGCG].

40. *See* Press Release, Day Pitney LLP, National Governors Association and Day Pitney Release Primer on Federal Cybersecurity Laws (Mar. 20, 2017), http://

work, originally published in February 2014, is a popular and proliferating framework. The voluntary framework was borne out of a collaborative process between industry, government, and academics with the intent of helping organizations reduce their cybersecurity risk.[41] Many states have already adopted the NIST Framework, including Virginia, Pennsylvania, Mississippi, Idaho, and New York.[42] In February 2016, then-California Attorney General Kamala Harris released the 2016 Data Breach Report. The Report pointed to the Center for Internet Security's Critical Security Controls as a "minimum level of information security," saying that the "failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."[43] This sparked speculation that the Critical Security Controls standard might spread beyond California.[44]

Although the regulatory environment in which state and local governments operate will continue to develop in the coming years, it is important that government actors who are not cybersecurity experts familiarize themselves with key cybersecurity concepts now and begin to apply them to their decision-making. As cybersecurity cannot be entirely outsourced successfully, it is important for decision makers to embrace a set of guiding principles to help them frame and consider the possible implications of their innovations and decisions. This is of added importance because checklists and compliance regimes may arrive slowly or unevenly and may even be poorly suited to the actual goal of improving cybersecurity posture.

A. CIA Framework

The classic Confidentiality–Integrity–Availability (CIA) triad offers a framework through which to consider security risks. The CIA framework is the classic information security triad that frames the goals of a security controls regime, ensuring that they enable the con-

---

www.daypitney.com/news/2017/03/20-nga-dp-primer-federal-cyber-laws [https://perma.unl.edu/L5X4-WRVS].

41. Ann Killilea & Amy C. Pimentel, *Where Are We Now? The NIST Cybersecurity Framework One Year Later*, McDermott Will & Emery (May 4, 2015), https://www.mwe.com/en/thought-leadership/publications/2015/05/where-are-we-now-the-nist-cybersecurity-framewor__.

42. *NIST Releases Update to Cybersecurity Framework*, Nat'l Inst. Standards & Tech. (Jan. 10, 2017), https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework [https://perma.unl.edu/P5QL-A226].

43. Kamala D. Harris, Cal. Dep't of Justice, California Data Breach Report, at v (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf [https://perma.unl.edu/FRW6-XDNR].

44. Paul Otto & Brian Kennedy, *"Reasonable Security" Becomes Reasonably Clear to the California Attorney General*, Hogan Lovells (Mar. 1, 2016), http://www.hldataprotection.com/2016/03/articles/cybersecurity-data-breaches/reasonable-security-becomes-reasonably-clear [https://perma.unl.edu/6YYP-TEEM].

fidentiality, integrity, and availability of information. "Confidentiality" means that the information is only accessible by those authorized to access it; "integrity" means that the information cannot be altered without detection; and "availability" means that the information is accessible when it is meant to be accessible.[45] The triad is often discussed in the context of specific security controls, but more broadly, it is a useful way to evaluate innovation before execution.

For a non-cybersecurity-expert government employee, understanding the CIA framework and applying it to the work of digital government innovations could naturally lead into a later conversation about, for example, access controls. Part III introduced three broad objectives that governments may have as they introduce digital technology into citizen interface—increasing access to content, digitizing some part of the service loop, and expanding or creating government functions. Section IV.B. discusses each trend through the CIA-framework lens to demonstrate how the framework can generate questions and frame concerns. The goal is not to create a comprehensive checklist for state- and local-government actors but rather to demonstrate the utility of such a framing device that could naturally form the starting point of such a checklist, while honoring the relevant expertise of non-cybersecurity-savvy government actors. With each trend, government officials should ask: (1) What are the threats to the confidentiality, integrity, and availability of this service; and (2) How can government officials be prepared for these threats?

These are not questions for a distant future but rather for an urgent present and recent past. Americans increasingly interact with their government online. A 2010 Pew survey found that eighty-two percent of Internet users, or sixty-one percent of all American adults "looked for information or completed a transaction on a government website in the twelve months preceding this survey."[46] Similarly, findings from a 2015 Pew study "generally suggest more Americans are using the government's online resources over time."[47] The following subsections will apply the CIA triad to these trends and offer questions to consider in light of these trends.

---

45. J.J. Stapleton, Security Without Obscurity: A Guide to Confidentiality, Authentication, and Integrity 57, 169 (2014). There have been many efforts to update and otherwise augment the classic triad to include themes like authentication, privacy, and nonrepudiation. Though those efforts are worthwhile, this classic triad is a sufficient and useful starting point.

46. Aaron Smith, *Government Online*, Pew Res. Ctr. (Apr. 27, 2010), http://www.pewinternet.org/2010/04/27/government-online [https://perma.unl.edu/BG4E-7W3M].

47. John B. Horrigan & Lee Rainie, *Connecting with Government or Government Data*, Pew Res. Ctr. (Apr. 21, 2015), http://www.pewinternet.org/2015/04/21/connecting-with-government-or-government-data [https://perma.unl.edu/W4LS-H8AG].

B. Applying the CIA Framework

1. Trend 1. Increasing Access to Information

Confidentiality. Governments that are increasing access to information quickly discover that some information is intended to be broadly accessed and some intended to be kept private. The driving factor of many state and local efforts is to open up more information to the public. Consequently, at first thought, confidentiality might not seem to be a primary concern. But while confidentiality might not be a major concern for information intended to be widely consumed, such as announcements alerting the broader public to an emergency, some data may be accompanied by information not intended to be widely consumed.

A 2017 report titled *Open Data Privacy*, from Ben Green at Harvard's Berkman Klein Center, highlights these very concerns. Green uses "privacy" instead of "confidentiality" as it is used here. The report begins with the premise that Personally Identifiable Information (PII) has become a technically meaningless concept because of the abundance of information collected about individuals by various sources, the archiving potential of the Internet, its increasing algorithmic power, and the unique mechanism of public-records laws that compel the release of certain specific information upon request. Simply put:

> Because so much data is now available from a wide variety of sources, and because databases can be manipulated and combined in complex and unpredictable ways, information that might not be deemed PII can lead to the identification of a specific individual and enable inferences to be made about that individual.[48]

With this new reality, the authors contend that the traditional focus on removing PII from datasets is misguided, or at least an incomplete approach. The report offers a series of recommendations for cities and other groups aiming to publicly release data. Among the recommendations are to consider privacy at every stage of the data lifecycle (not just at the moment of releasing open data) and to "[d]evelop operational structures and processes that codify privacy management throughout the City."[49]

Integrity. When it comes to the integrity of information, government actors should ask themselves how vulnerable published information is to being changed by an outside source—with or without detection—and what would be the impact of such manipulation.

The 2016 U.S. election also previewed another threat to the potential integrity of information: the purposeful spread of disinformation.

---

48. BEN GREEN ET AL., OPEN DATA PRIVACY 3 (2017), https://dash.harvard.edu/bitstream/handle/1/30340010/OpenDataPrivacy.pdf?sequence=5 [https://perma.unl.edu/B7M6-2N5P].

49. *Id.* at 5.

While disinformation tactics are far from new, and a growing body of research explores its impact, this conversation also affects states and localities as they increase access to information. These actors ought to consider how their increased attempts at communicating information to citizens online makes citizens more vulnerable to disinformation campaigns. Agencies can address this threat by implementing procedures and access controls that make it harder for hackers to gain access to government social media accounts and spread disinformation, or by considering ways to mark accounts as "authentic" to the viewing publics to make them more difficult to imitate.

New York State's guidelines for secure use of social media moved in this direction with guidelines like "Do not use the same passwords for social media sites as are used to access State resources," and recommend technical controls designed to mitigate risks, such as URL and IP filtering, and intrusion detection and prevention systems.[50] Similarly, Digitalgov.gov offers a Readiness, Recovery, Response toolkit for social media vandalism.[51]

More broadly, preventing the manipulation of information is an increasingly urgent matter, where emphasis has previously been on assuring confidentiality and availability of information. Director of National Intelligence James Clapper emphasized this point when testifying before Congress in September 2015, warning:

> In the future . . . we might also see more cyber operations that will change or manipulate electronic information in order to compromise its integrity (i.e., accuracy and reliability) instead of deleting it or disrupting access to it. Decisionmaking by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving.[52]

Consider this: If government decisions are made based off long-recorded data, and that information is altered or is made incomplete, what is the impact? The consequences could range from mild confusion to chaos. The 2016 U.S. election raised concerns for many about the security of many parts of our election system. Tampering with voter-registration logs such that names of registered voters go missing or become unrecognizable is an example of a high-impact hack that compromises the integrity of information. One could also imagine a scenario in which long-recorded data about outcomes of a policy inter-

50. IT BEST PRACTICE GUIDELINE NO. NYS-G10-001 § 3.2 (OFFICE OF INFO. TECH. SERVS., STATE OF N.Y. 2014), https://its.ny.gov/sites/default/files/documents/secure-use-of-social-media.pdf [https://perma.unl.edu/L6AS-YB4M].

51. *Readiness, Recovery, Response: Social Media Cyber-Vandalism Toolkit*, DIGITALGOV, https://www.digitalgov.gov/resources/readiness-recovery-response-social-media-cyber-vandalism-toolkit [https://perma.unl.edu/Y9WC-E8ZK].

52. *Worldwide Cyber Threats: Hearing Before the H. Permanent Select Comm. on Intelligence*, 114th Cong. 5 (2015) (statement of James R. Clapper, Director, National Intelligence), https://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf [https://perma.unl.edu/LDR2-A3U7].

vention were altered in a way that influenced decisions made about future allocation of funds.

Availability. In many spaces, though certainly not everywhere, open data in many spaces is something of a novelty. In this environment, temporary unavailability might not be so concerning, but going forward, attitudes around open data and other forms of information shared by government to the public might shift such that availability of certain types of information becomes central to core functions.

Looking forward, what is the impact of nonavailability of open data? Outside of open data, state and local officials should ask themselves such questions as: What happens if a social media page goes down in the wake of a distributed denial-of-service (DDoS) attack? What is the impact of that sudden absence of information in a crisis? How do people respond in the absence of this form of communication? Again, these are not concerns for the distant future. DDoS attacks against state websites are an increasingly popular tool for hacktivists during times of civil unrest.[53] During the water crisis in Flint, Michigan, and in the wake of the police killing of Freddie Gray, a hacktivist group called "Anonymous" directed DDoS attacks, temporarily taking down the state website of Michigan and the city website of Baltimore.[54]

2. Trend 2. Digitizing Government Service Loop

Confidentiality. When information is being exchanged, the information has to be stored somewhere, even if only temporarily. Is that information stored confidentially? The paper version may be stored in a filing cabinet, with or without a secure physical lock or code. The security analogy in a digital context is the strength of encryption and key storage.

Other key questions involve the relationship between data and third parties. Is data hosted in the cloud, or is it in the hands of a third party? What is the relationship with third parties, and how are they maintaining the confidentiality of information being collected and used? What are the consequences of confidentiality that is compromised, and what is the likelihood of that happening?

Integrity. Again, government actors should ask whether information is stored in the cloud or is otherwise in the hands of a third party. What is the relationship with the third party, and how are they main-

53. Ian Duncan, *City Faced Cyberattacks Amid Chaos and Unrest on the Streets*, BALT. SUN (July 31, 2015), http://www.baltimoresun.com/news/maryland/sun-investigates/bs-md-ci-cyber-riot-20150731-story.html [https://perma.unl.edu/EYL7-Z2NC].

54. Amanda Emery, *State Confirms "Cyber Attack" Similar to One at Flint Hospital*, FLINT NEWS (Jan. 22, 2016), http://www.mlive.com/news/flint/index.ssf/2016/01/state_confirms_cyber_attack_si.html [https://perma.unl.edu/E4FR-ANRP].

taining the integrity of information collected? One might also think about the integrity of the new process—does it work the way it is meant to? Does a form that is sent electronically to a department actually end up there, or does it end up elsewhere?

Availability. What happens when a system is not available? Has the system done away entirely with a paper process, and what does that mean for system unavailability? What precautions could be taken to prepare for the unavailability of the process, and how does one weigh the risks against the benefits of going paperless?

3. Trend 3. Expanding or Creating Government Functions

The activity of expanding or creating government functions is sparse, and as a result, the questions are broader and more speculative. Overall, until the field develops further, these considerations are very similar to those that arise in digitizing the service loop.

Confidentiality. Similar to the digitizing of a service loop, does the information captured by the creation and expansion process stay accessible only to those authorized to access it?

Integrity. How does one ensure both that the process maintains integrity—that it functions the way it is meant to function—but also that information captured by the process cannot be altered without detection?

Availability. As a new function without a neat offline analog, how will citizens come to rely on this process, and what would the consequences be of nonavailability?

The CIA framework may be especially helpful in the face of these unclear, yet rapidly innovating programs. While the specific digital-governing function of the future may be unknown, it is still possible to probe whether the confidentiality, integrity, and availability of the data or service are assured with each new innovation and to use that framework to try to understand risks that accompany innovation.

More broadly, a central question is: How will the government verify citizen identity in cyberspace? Any initiative in this space is likely to require a method that the government can create or verify a trusted digital identity. The process by which this develops is a topic of much debate, including by a NIST working group, and is the subject of the National Strategy for Trusted Identities in Cyberspace.[55]

Other questions in this area concern civic-tech initiatives that create digital assets that are largely owned or operated by citizens but have a reporting or feedback option for government actors to play a

55. THE WHITE HOUSE, NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE: ENHANCING ONLINE CHOICE, EFFICIENCY, SECURITY, AND PRIVACY 8 (2011), https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf [https://perma.unl.edu/FXE3-RV6K].

role. How can, and should, the government be involved in setting up rules for the road when they are not primary architects of the system? This is another area for consideration. Finally, to what extent are these new services being carried out with the assistance of a third party? What rules govern the relationship between the government and the third party? The most recent NIST Cybersecurity Framework draft includes an expanded focus on third-party risk, which reflects a growing dependence on third-party actors.[56]

V. INNOVATIONS IN E-GOVERNMENT: CASE STUDIES

A. New Jersey: Open Data Initiative

As is often the case, open-data initiatives in government precede formal declaration. They are piloted and respond to the needs and demands of communities before being enshrined in state law. This was the case in New Jersey, where open data efforts had been underway for a few years. The State already hosted data sets on its open-data site, data.nj.gov, and various state agencies also had their own online open-data portals.

In February 2017, the New Jersey legislature passed the Open Data Initiative, which codified and authorized the role of Chief Data of Officer into state law.[57] The role was filled by then-Deputy Chief Technology Officer Liz Rowe. Rowe's duties were to establish standards and procedures around open data in New Jersey. These standards include security standards around tampering with data to ensure its integrity.[58]

In New Jersey, the Chief Data Officer reports to the Chief Technology Officer, David Weinstein. In an interview discussing the Open Data Initiative, Weinstein said that it started out mainly focused on financial data so the public could see how the government was spending. Weinstein indicated that Chief Data Officer Liz Rowe thought about the Open Data Initiative in the context of governance and in terms of establishing a data-governance enterprise model across the various branches of government. In the optimal end state, according to

56. *NIST's Draft Update to Cybersecurity Framework Focuses on Third-Party Vendors and the Cost-Effectiveness of Cybersecurity Programs*, CADWALADER, WICKERSHAM & TAFT LLP (Feb. 1, 2017), http://www.cadwalader.com/resources/clients-friends-memos/nists-draft-update-to-cybersecurity-framework-focuses-on-third-party-vendors-and-the-cost-effectiveness-of-cybersecurity-programs [https://perma.unl.edu/L29G-WM25].

57. Colin Wood, *New Jersey Launches Open Data Initiative, Appoints Chief Data Officer*, STATESCOOP (Feb. 6, 2017), http://statescoop.com/new-jersey-launches-open-data-initiative [https://perma.unl.edu/Y9P6-K25P].

58. Colleen O'Dea, *One-Stop Online Source for All Data to Make Government in NJ More Transparent*, NJ SPOTLIGHT (Feb. 7, 2017), http://www.njspotlight.com/stories/17/02/06/one-stop-online-source-for-all-information-to-make-nj-government-more-transparent [https://perma.unl.edu/JZ56-F3AM].

Weinstein, every agency would have a qualified data officer of its own who works with the Chief Data Officer.

Though open-data efforts were already underway, in New Jersey, the open-data legislation and the establishment of a Chief Data Officer ensured that e-government innovation did not get too far ahead of a formal mechanism for coordination and oversight. For New Jersey, having a Chief Technology Officer and Chief Data Officer helps to ensure that at least some cybersecurity-related concerns are considered in the early stages of innovation.

B. Boston: Mayor's Office of New Urban Mechanics

New Urban Mechanics is the oldest so-called innovation office within municipal government in the United States. It was founded within the City of Boston Mayor's Office in 2010 and was designed to "leverage technology and innovation to improve the quality of City services and to strengthen the relationship between citizens and the City to promote 'peer-produced governance.'"[59]

Their first big project, Citizens Connect (now called Boston311), which launched in 2009, allows community members to report issues directly to government and track responses.[60] Its current program director, Stephen Walter, spoke with me to outline how the department's focus has evolved. Walter described the shifting focuses of MONUM over time in terms of the trends I presented—increasing access to relevant content, digitizing services, and expanding or creating new city services. According to Walter, MONUM primarily focused on the first two objectives in the beginning. Back in 2010, in addition to what is now Boston311, the department concentrated on digitizing government services, predominately by opening up city services to new audiences through online services. In addition, MONUM is also thinking about how to open data sets up to nonspecialists. However, now and going forward, MONUM is thinking much more about the third function: how to expand or create new government functions.

As a department specifically dedicated to innovation, MONUM is uniquely positioned in comparison to other offices as it experiments, takes risks, and has the ability to fail. According to program director Walter, MONUM has "a unique privilege in that [its] mandate is about taking risks that other departments simply can't do, whether

59. Ben Schreckinger, *Boston: There's an App for That,* POLITICO MAG. (June 10, 2014), http://www.politico.com/magazine/story/2014/06/boston-theres-an-app-for-that-107661 [https://perma.unl.edu/4DSB-XBT9].

60. Nick Carney, *Citizens, Connected*, ASH CTR. FOR DEMOCRATIC GOVERNANCE & INNOVATION (May 21, 2013), http://datasmart.ash.harvard.edu/news/article/citizens-connected-245 [https://perma.unl.edu/UXB6-XUJ8].

it's not having the staff capacity or some other barrier."[61] Furthermore, the department understands its influence: the way it does things often trickles into other programs in Boston and elsewhere. Consequently, it pays close attention to its processes up front, being mindful of what may spread elsewhere.

This trickle effect, as well as its specific focus on innovation, explains in part why MONUM gives serious thought to cybersecurity-related issues up front. In discussing the sensitivity of Personally Identifiable Information (PII), which would arise under *confidentiality* of the information-security triad, Walter said that MONUM actively discusses these concerns internally. He explained that, where many other groups might not consider a detail like a MAC address to be PII, a group like the ACLU might take a different stance. What right does a person have to the data their body generates in a public right of way? MONUM has been considering questions like this over the past year. In Boston, having an office dedicated to innovation is a mechanism that helps to ensure that MONUM can balance many interests—accessibility, innovation, and renewing faith in government, among others—while thinking critically about at least some aspects of cybersecurity.

VI. CONCLUSION

In addition to being a technical problem, cybersecurity is a human problem. A key element of the latter problem is one of communication. The language and conceptual frameworks used by key actors vary in ways that can hinder mutual efforts. The expanding cybersecurity-threat landscape is especially challenging for state and local governments that often operate in low-resource environments. Those on the front lines of state- and local-government innovation make decisions responding to various pressures—budgetary and otherwise. These governments seize new opportunities to redefine their relationships with their citizens. In the absence of a clear regulatory framework or checklist, such actors may continue to innovate without thorough consideration of relevant cybersecurity concerns. The absence of such consideration does not necessarily make a decision unwise, but state and local government actors who are invested in protecting their systems and citizens would benefit from embracing simple rubrics to help frame their decisions. The CIA framework is well suited to do just that. When applied to the three broad trends in the ways governments are interfacing with citizens, it yields useful results. The framework offers a strong conceptual foundation for sector-specific and technical conversations that may later emerge.

61. Telephone Interview with Stephen Walker, Program Dir., City of Bos. Mayor's Office of New Urban Mechs. (Mar. 9, 2017).