Appendix 3: A New Approach to Regulation

A new agile approach to regulatory oversight is required to deal with the fast-paced nature of digital technology and its marketplace impact. In broad terms, such an approach should be built around the common law-derived principles of duty of care and duty to deal and oriented towards risk management rather than micromanagement. To accomplish this, the Digital Platform Agency should identify risks to consumers and competition and respond through the initiation and approval of cooperatively development and enforceable behavioral codes, accompanied by enforcement authority. Where such cooperative activity does not produce results acceptable to the DPA, the agency will act on its own.

Top-down, rules-based management—for both companies and governments—was possible because the pace of change was slower than today.

Moving from Industrial Era-Style Oversight

As Appendix Two makes clear, the regulatory agencies of the federal government were created in response to the effects of the industrial economy. In so doing, the structure and management of these agencies adopted the prevailing practices of the industrial era. Thus, at a time when industrial management was a top-down, rules-based bureaucracy, the agencies created to oversee industrial activity adopted a similar approach.

Such top-down, rules-based management—for both companies and governments—was possible because the pace of change was slower than today. The pattern of new technology adoption historically experienced a "diffusion lag" with adoption coming long after invention.[84] Stanford professor Paul David illustrated this phenomenon in a study of the impact of electrification on industrial production.[85] He noted, for instance, that factories didn't reach 50% electrification until four decades after the first central power station opened. Such a slow-paced adoption of new technology was reflected within corporate management structures, as well as in the government's oversight of that management. When developments progressed slowly, such oversight, whether by management or by government, was sufficient.

84 Diego Comin and Bart Hobijn, *An Exploration of Technology Diffusion,* AM. ECON. REV. 100 (Dec. 2010), 2031–2059, https://www.dartmouth.edu/~dcomin/files/exploration_technology.pdf.

85 Paul David, *The Dynamo and the Computer: An Historical Perspective On the Modern Productivity Paradox,* AM. ECON. REV. 80 (1990), 355–61, https://www.researchgate.net/publication/4724731_The_Dynamo_and_the_Computer_An_Historical_Perspective_On_the_Modern_Productivity_Paradox

The current pace of technology innovation and adoption is far from slow-paced. As a result, digital era companies have abandoned rigid, rules-based bureaucratic management. The diffusion lag has been replaced with "blitzscaling" which emphasizes large magnitude increases in development, delivery, and adoption in a short amount of time.[86]

In place of rigid management practices, digital companies follow agile practices that allow them to constantly react and evolve in the face of new developments. The classic example of such agility is the frequent updating of software for devices and applications. Every time Apple updates the iPhone software, Microsoft updates Windows, or the Weather Channel updates its smartphone application, agile software management is being practiced. If the DPA is to keep abreast of this rapid pace of change, it, too, must become agile in its applications of the statute.

This is a process designed to produce mandatory behavioral standards that are more measurably effective than blindly trusting the market and best practices, yet because of the companies' involvement, more agile.

Such agility should be based around combining the public participation underpinnings of the current regulatory process with a new model based on supervised but cooperative industry-public development of enforceable behavioral codes. The new process is one of cooperative engagement in order to create policies that are more dynamic than traditional regulation. Make no mistake, however, this is a process designed to produce mandatory behavioral standards that are more measurably effective than blindly trusting the market and best practices, yet because of the companies' involvement, more agile.

From Micromanagement to Risk Mitigation

The adverse effects of the amazing products and services produced by digital platform companies have- too often been accompanied by a lack of consideration of the impact on the public interest, let alone any attempt to mitigate those adverse effects. The wholesale siphoning of personal information proceeded without consideration of its broader impact on the privacy rights of individuals. The subsequent hoarding of that data proceeded without consideration of mitigating its impact on other marketplace and media participants, and thus on competitive dynamism. Similarly, lax security has too often permitted the exfiltration of personal information.

Of course, it is possible to paint a picture where the platform companies ignored the consequences of their actions by *design.*[87] The rewards of such behavior are great; what economists describe as monopoly rent: high prices and high profits. Whether the consequences were intentional or accidental, however, the results are the same: adverse consequences for consumers and competition. Such results demand mitigating solutions.

86 REID HOFFMAN, BLITZSCALING: THE LIGHTNING-FAST PATH TO BUILDING MASSIVELY VALUABLE COMPANIES, Penguin Random House (2018).

87 The disinclination of large firms to cooperate with smaller rivals has been extensively studied. See, e.g., Stanley M. Besen & Joseph Farrell, *Choosing How to Compete: Strategies and Tactics in Standardization,* 8 J. ECON. PERSPECT. 117, 126–29 (1994); CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY, 197 Harvard Business School Press (1999); Daniel L. Rubinfeld & Michal S. Gal, *Access Barriers to Big Data,* 59 ARIZ. L. REV. 339, 367 (2017).

Earlier efforts at regulating the effects of new technologies often evolved into so-called "utility regulation" where the behavior of companies was precisely regulated in an effort to mitigate adverse effects. Such micromanagement was possible when new developments were slower paced and experiencing the diffusion lag.

The fast pace of the digital era requires a creative new approach to regulatory oversight. Old style regulation can be counterproductive if it prioritizes dictating detailed procedures over boundary-expanding innovation. Yet—and this is the key rationale for the DPA—the broad definition of consumer welfare, and market competition cannot be allowed to become continuing casualties in a digital economy.

The fast pace of the digital era requires a creative new approach to regulatory oversight.

The common law-derived principles of duty of care and duty to deal form the foundation of the DPA's substantive mandate. These concepts have provided the starting point for the derivation of American laws and regulations applicable to particular industries throughout the country's history. Enacting the principles into law will supply a reliable basis for the development of obligations applicable to systemically important digital platforms, even as technology and market activities evolve.

Consistent with the underlying agile risk management approach recommended here, the objective of Congress should be to make the obligations as general and flexible as circumstances permit. The dynamic nature of the digital enterprises calls for a lighter regulatory touch based on identifying and mitigating significant risks rather than directing specific operational behaviors.

The operation of the DPA is designed to attack and mitigate adverse effects without the necessity to micromanage the processes leading to those effects. Such risk management is accomplished through identification of the risk, the design of actions to mitigate that risk through a cooperative public-private Code Council – all overseen, ultimately approved by, and enforced by the DPA.

The DPA, thus, is responsive to the arguments of the digital companies that regulatory intrusion to dictate corporate management practices can negatively impact innovation. At the same time, the DPA's adherence to and enforcement of a duty of care and duty to deal principles provides the focused public interest protections that currently are absent.

General Operations of the DPA

The DPA should have many of the common characteristics of traditional regulatory agencies. For instance, a multi-member commission in structure with a staff of subject matter experts that adheres to the Administrative Procedure Act (APA). The agency will need experts in engineering, computer science, application development, economics, as well as the law relative to these fields. The selection of commissioners should pay particular attention to appointing individuals with not just subject matter expertise, but also management experience and independent decision-making.

What sets the DPA apart from traditional agencies is twofold: (1) its combination of agile regulatory operations with the kind of public participation required in the APA, and (2) its focus on concerns that flow from network effects, the power of data collection and exploitation, and the winner-take-all nature of digital platforms.

Stated differently, the DPA embraces a variant of the familiar industry standards development process while retaining traditional rulemaking and enforcement regulatory tools should the standards process prove insufficient. Within the digital ecosystem, such a standards-setting process is widely practiced to good effect. That is not to say that the process is untroubled as corporate self-interest can lead to material disputes.[88] But the ultimate success of the standards development process in terms of industry progressiveness and material advancement is beyond dispute.

the DPA embraces a variant of the familiar industry standards development process while retaining traditional rulemaking and enforcement regulatory tools should the standards process prove insufficient.

The DPA's hybrid private-public process is designed to result in cooperatively developed standards subject to government enforcement. As a backstop (as well as an incentive), if the cooperative process is not successful, an alternative process enables the DPA to promulgate standards on its own. In both cases, due process obligations are respected, but within deadlines appropriate to the dynamic nature of digital technology and the services it enables.

In a genuine sense, then, this is not new. As the following discussion indicates, our country, and others, have relied upon informed industry experts to develop practical solutions to challenges and opportunities arising out of their industries, and continue to do so today. In many circumstances, because of the manifest public importance of the resulting standards, many have been made mandatory. Yet, the manifest advantages of producing to a standard have also led to widespread acceptance without any requirement to bring forward the government's coercive power. In the case of systemically important platforms, by virtue of their market power or their essentiality to society or both, it is necessary to impose safeguards on both the process of deriving certain standards and on their faithful implementation.

The argument digital companies have traditionally used against oversight is that the rigidity of old-style regulation stifles the "permissionless innovation" that has characterized digital technology. When efforts are made to avoid such consequences through the articulation of broad behavioral standards, the companies complain about "regulatory uncertainty." Opposition to both rigid as well as flexible regulation, of course, results in no regulation at all.

The DPA overcomes those concerns and the current absence of behavioral policies by appropriating practices long utilized by the commercial sector: industry codes. In response to rapidly changing technology, the DPA's process creates an operational structure in which enforceable regulatory codes can evolve with technology. In place of top-down government dictates of corporate activities, the DPA involves the companies as well as other credentialed experts directly in the Code development process. Should the Code process fail, however, the agency itself retains authority to decide an issue.

Precedents in the U.S. (Non-Governmental)

In 1895 representatives of the manufacturers of fire suppression sprinklers and insurance companies met in Boston to resolve the inconsistencies among sprinkler

88 To take a particularly contentious example, see FTC v. Qualcomm, Inc., 411 F.Supp.3d 658 (N.C. Cal. 2019), app. docketed and stay granted, 935 F.3d 752 (9th Cir. 2019).

and piping installations.[89] The result was a common code and the creation of the National Fire Protection Association (NFPA).[90] Today there are over 275 NFPA codes and standards ranging from fire codes, to the National Electric Code, to the standards for safety matches. The NFPA is an example of a self-regulatory organization (SRO) that operates with the endorsement of the government, and often through enforcement by government.

In response to rapidly changing technology, the DPA's process creates an operational structure in which enforceable regulatory codes can evolve with technology

Activities dealing with public health and safety have been in the forefront of such SRO-government alliances. The American Society of Civil Engineers, for instance, has codes for over 60 different activities, ranging from minimum building design loads, to flood resistance, to standards for people movers. These codes, in turn, have become the standards for government requirements and inspections.[91]

Technology-based businesses are similarly governed by collectively developed standards, but without the governmental enforcement aspect. The internet itself is made possible by a set of standards that allow otherwise incompatible networks to work as one. Smart home technology companies that use the internet are developing standards to assure device compatibility.[92] Telecommunications networks have for a long time relied on cooperatively developed common standards; everything from plug-in jacks to the new 5G networks are based on industry-wide agreement.

Industries have also used codes and standards to respond to issues raised by public policymakers. One of the authors of this paper was involved in establishing the Consumer Code for Wireless Service to govern the consumer-facing issues confronted by the mobile phone industry.[93] The purpose of that Code was to demonstrate industry self-oversight as an alternative to regulation. Years later, in his role as a regulator, the author encouraged the industry to amend the Code to address a specific consumer protection issue, and the industry reacted responsibly. Both experiences were informative of the recommendation in this paper. [94]

These are the proof of the concept for the DPA. Industry expertise, if encouraged to address a public policy problem, has proven capable of producing satisfactory results. Underpinning such codes, of course, is the realization that something beyond goodwill is essential to such an undertaking's success.

A great advantage of such industry codes is their flexibility to reflect operational and technical realities in a timely manner. Typically, the industry uses a structure such as a code council to develop the standards based upon prevailing technological capabilities and other practical issues. The codes also offer the ongoing opportunity for industry or other input to trigger updating to reflect new developments.

89 *History of the standards development process,* National Fire Protection Association (n.d.), https://nfpa.org/codes-and-standards/standards-development-process/how-the-process-works/history-of-standards-development.

90 *All codes & standards,* National Fire Protection Association (n.d.), https://www.nfpa.org/Codes-and-Standards.

91 *Codes & Standards,* American Society of Civil Engineers (n.d.), https://www.asce.org/Codes-and-Standards/Codes-and-Standards/.

92 Zachary Comeau, *Big Tech Is Developing Standards For Smart Homes,* MY TECH DECISIONS (Dec. 20, 2019), https://mytechdecisions.com/facility/big-tech-is-developing-standards-for-smart-homes/.

93 *Id.*

94 The issue was the unlocking of mobile devices, once paid for, to permit usage on a competitive network.

A challenging part of creating and managing a voluntary industry code is that it is only as strong as the industry's weakest link. The innumerable hours of interindustry negotiations necessary to develop the Wireless Code, for instance, demonstrated that the search for the necessary industry consensus meant that each participant had a veto. Once a code is adopted, a new challenge arises surrounding its enforcement. Just what happens when a company thumbs its nose at the code? In fact, on the example of the industry being asked to amend the Wireless Code, the majority of the companies—including all the major companies—respected the additional provision but were unhappy when it was not universally adopted in practice.

Today there are over 275 NFPA codes and standards ranging from fire codes, to the National Electric Code, to the standards for safety matches.

Since 1895 industries have looked to self-developed codes for both safety and coordination. Many, like the National Electric Code, are subsequently adopted into law and governmentally enforced. Unfortunately, for consumer-facing digital platforms such an industry-developed, governmentally overseen code does not exist. The focus of the DPA should be to overcome this shortcoming through a government-convened Code Council of industry and public representatives, accompanied by appropriate agency oversight of the process and enforcement of the outcome.

Precedents in the U.S. (Governmental)

The National Fire Protection Association and American Society of Civil Engineers are self-regulatory organizations whose codes are often enforced by government. There are also SROs that assume regulatory authority from the federal government.

The North American Electric Reliability Corporation (NERC) was formed by the industry in 1968 to promote a reliable and adequate energy supply to electric utilities. Rather than binding "standards," NERC produced voluntary industry "policies." The 2003 Northeast power blackout, however, demonstrated the need for something more than voluntary "policies."

The Energy Policy Act of 2005, passed in response to the blackout, mandated the creation of an Energy Reliability Organization (ERO) to develop and enforce compliance with mandatory reliability standards. The Federal Energy Regulatory Commission (FERC) appointed NREC to be that ERO and gave it the responsibility of developing and enforcing these mandatory rules. In July 2006, NERC filed its first mandatory Reliability Standards with FERC.

The Financial Industry Regulatory Authority (FINRA) is another SRO with governmentally delegated and supervised authority. FINRA regulates brokerage firms and exchange markets through registration and examination to determine compliance with applicable financial market laws. FINRA also oversees the arbitration of disputes between consumers and member financial institutions, as well as industry advertising practices.

The Securities and Exchange Commission (SEC) oversees FINRA's application of the statutes and SEC rules, including, where applicable, proposing FINRA rules. Typically, the process begins with FINRA filing a proposed rule with the SEC, publication of the proposal in the Federal Register and receipt of comments. The SEC reviews the proposal, the public comments, as well as FINRA's input prior to a determination whether the proposed rule is consistent with the requirements of the Exchange Act governing the financial markets. Under the Dodd-Frank Wall

Street Reform and Consumer Protection Act, the SEC's authority to directly disapprove a rule or to institute proceedings to determine whether to disapprove a proposed rule was expanded.

The Dodd-Frank Act also mandated a review of FINRA's activities by the Government Accountability Office (GAO). The review found a need for the SEC to "enhance its oversight of FINRA."[95] Among the findings was "the level of SEC's oversight…has varied." Improvements were recommended for a "process for examining FINRA's reviews" of its policies as well as the development of a risk-management framework to evaluate the effectiveness of FINRA's rules.

Since 1895 industries have looked to self-developed codes for both safety and coordination.

The DPA builds on these experiences, beginning with the establishment of a legal framework rooted in common law-derived principles and expressed in a code construction process applicable to the consumer-facing digital marketplace. The Code Council's decisions, once affirmed by the DPA, will be agency enforceable decisions.

Precedents Elsewhere

The idea of industry-developed, government-overseen digital practices has a prominent example in the U.K. The regulator that put the initial plan in place is presently expanding its concept into other areas as well.

The U.K.'s Open Banking[96] Initiative was ordered for the country's nine largest financial institutions by the Competition and Markets Authority (CMA).[97] The CMA itself was created in 2012 by merging two predecessor agencies in order to strengthen competition protection activities. The CMA is a non-ministerial agency akin to the independent agencies of the U.S. government.

The purpose of the open banking order was to increase competition in financial services by allowing consumers to request that the data the banks held about them would be shared with new competitors, both smaller banks as well as online services. In 2016, after the previous "My Data" initiative failed because of industry intransigence, the CMA ordered the covered banks to create, fund and operate the Open Banking Implementation Entity (OBIE).[98]

The OBIE was required to establish standards for mandatory open Application Programming Interfaces (APIs) that would allow different entities to access and interface with the banks' databases. The OBIE is overseen by a Trustee appointed by the CMA. The Trustee is empowered to take "proportionate and reasonable" actions to establish standard data structures, security architecture, and other practices necessary for non-affiliated companies to utilize the customer's information.[99]

95 U.S. Government Accountability Office, Securities Regulation: *Opportunities Exist to Improve SEC's Oversight of the Financial Industry Regulatory Authority* (Report to Congressional Committees) (May 2012), https://www.gao.gov/products/GAO-12-625.

96 Bill Roberts, *Celebrating the first anniversary of Open Banking, Competition and Markets Authority* (Jan. 11, 2019), https://competitionandmarkets.blog.gov.uk/2019/01/11/open-banking-anniversary/.
https://www.gov.uk/government/organisations/competition-and-markets-authority.

97 *Id.*

98 Open Banking, *About Us,* (n.d.), https://www.openbanking.org.uk/about-us/

99 Author interview with Imran Gulamhuseinwala, Trustee, Open Banking, Ltd.

The European Union has developed a similar open banking requirement for its member nations. This Payment Services Directive (PSD2) utilizes a more traditional top-down regulatory approach.[100] Under PSD2 the financial institutions are told what to do, but not how to implement it. As a result, there are no common standards for APIs or for the validation of companies with access to the data.

As of mid-2020 there are 90 banks that are not covered by the OBIE that nonetheless follow its practices in order that they, too, can participate in the shared data program. Open APIs became widely usable in the late summer of 2019. In the 12 months that followed, slightly fewer than 200 third party competitive service providers have been authorized to participate in the program and 70 are operational.[101]

Digital markets will only work well if they are supported with strong pro-competition policies.

The Open Banking Initiative was prominently featured in the March 2019 report by a U.K. government-convened Digital Competition Expert Panel chaired by former Chairman of the White House Council of Economic Advisors Jason Furman. The Johnson government's March 2020 Budget provided that "[t]o empower consumers and boost competition, the government will accept all six of the Furman Review's strategic recommendations for unlocking competition in digital markets."[102]

The conclusion of the Furman Review was that "digital markets will only work well if they are supported with strong pro-competition policies" but that traditional antitrust policies are a blunt instrument to achieving that goal. "The biggest gains," the report concluded, "will come from going beyond these [traditional] tools to focus on policies that actively promote competition, foster entry by competitors, and benefit consumers."

When it came to advertising-supported digital services, the Furman Review recommended creation of a "code of competitive conduct with the participation of stakeholders" similar to the Open Banking Initiative. Those stakeholders would be companies "deemed to have 'strategic market status,' in order to avoid creating new burdens or barriers for smaller firms."

In June 2019 the U.K. government announced plans to establish the Digital Markets Unit within the CMA.[103] The following December the CMA published an interim report seeking comments on the implementation of such activities.[104] A final report meant to guide implementing legislation, was published July 1, 2020.[105]

The conclusion of the final CMA report was that "these markets are so wide ranging and self-reinforcing that our existing powers are not sufficient to address them." The conclusion called for "a new regulatory approach" built around enforcement of "a code of conduct to govern the behavior of platforms with market power."

100 *Payment Services Directive,* Wikipedia (n.d.), https://en.wikipedia.org/wiki/Payment_Services_Directive.

101 Gulamhuseinwala interview, supra note 99.

102 *Budget 2020 Policy Paper,* U.K. House of Commons 121 (Mar. 11, 2020), https://www.gov.uk/government/publications/budget-2020-documents/budget-2020.

103 U.K. Prime Minister Theresa May, *London Tech Week.* (Opening speech) (Jun. 10, 2019), https://www.gov.uk/government/speeches/pm-speech-opening-london-tech-week-10-june-2019.

104 CMA Interim Report, *supra* note 22.

105 CMA Interim Report, *supra* note 14.

Initiation of the DPA Process

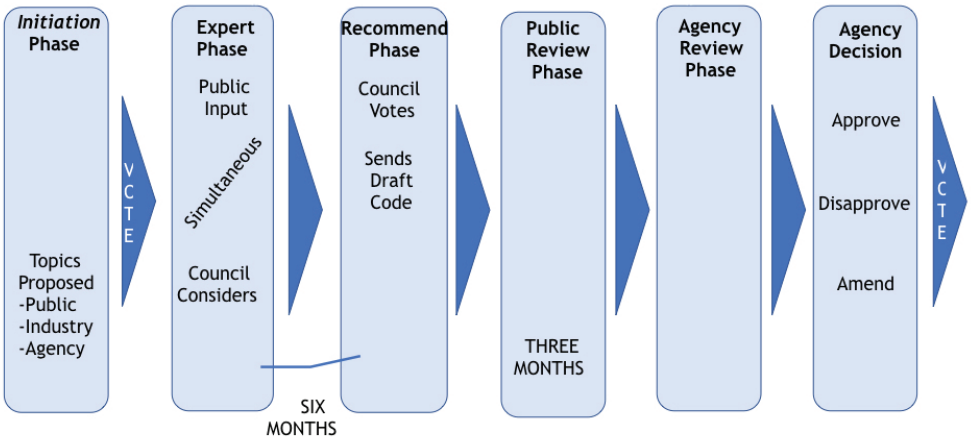
The DPA is first and foremost a regulatory agency charged with protecting consumers and competition. The innovative use of cooperatively developed codes is for the purpose of mitigating the traditional complaint of regulatory overreach and lack of agility, not the dilution of oversight.

The DPA is first and foremost a regulatory agency charged with protecting consumers and competition.

The DPA Code process can be initiated in three ways: (1) upon petition by the public or industry, (2) by a majority vote of the Code Council, or (3) by a majority vote of the DPA.

While it is likely that responsible members of the platform industry will recognize the necessity of certain actions, a necessary predicate to such self-realization is often the threat of independent regulatory action. Thus, the ability of the DPA to initiate rulemakings outside the Code process on its own initiative is an essential component of the new regulatory paradigm.

Workflow of a Digital Platform Agency



The Code Council

The heart of the DPA's new regulatory paradigm is the establishment of an industry/public/government Code Council charged with the responsibility of bringing forth for DPA approval or disapproval enforceable behavioral rules for affected companies. The Code Council does not itself have regulatory authority; its purpose is to supplement the traditional notice and comment rule-making of a federal agency with a process to develop behavioral codes that carry out the broad principles of the statute and are enforceable by the DPA.

The Code Council would be composed of members equally divided between industry representatives and representatives of the public. Each member would serve a staggered three-year term so that one-third of the Council rolls over an-

nually. Council members shall have demonstrated expertise in digital technology as well as its economic and social effects. Members will be expected to treat the Council in a manner similar to that of industry representatives on U.S. delegations to international conferences with individual obligations to unbiased, faithful service. The Council shall utilize the professional staff of the DPA.

The Code Council would be composed of members equally divided between industry representatives and representatives of the public.

The Chairman and Vice Chairman of the Council will rotate annually (i.e., one-year industry is chair and public is vice chair, the next year it reverses). The Council should formally meet not less than monthly with ongoing activities between meetings. These meetings will be transactional, not pro forma, meaning that the Council members will engage in public debate and discussion.

Code Council Procedures

The Council shall act through a multi-step process to develop the specifics of an enforceable Code to be recommended to the DPA:

- "Initiation Phase" based on inputs from the Code Council, the public, or the agency's own motion, the DPA votes to start a Code Council consultation.
- "Expert Phase" (effectively similar to a Notice of Inquiry) not to exceed six months during which the Code Council will examine and issue, and, if possible, propose a behavioral code. During this period, the Council will develop its own factual record. Included in this phase will be the submissions by any interested party—submissions that will be publicly disclosed.
- "Recommendation Phase" at the end of the Expert Phase—yet within its six-month timeline—when the Council forwards its recommendation and any relevant supporting material to the DPA. This submission may include, as appropriate, minority reports.
- "Public Review Phase" when the DPA, for a period of not to exceed three months, receives public comments on the recommendation—submissions that will be publicly disclosed.
- "Agency Review Phase" in which the DPA reviews both the Code Council's recommendation and public input.
- "Agency Approval, Disapproval and/or Amendment Phase" in which the DPA decides by majority vote whether to adopt, reject or amend on a line item basis the Code Council's recommendation. Regardless of which action is taken, the agency shall provide its rationale to the public.

The use of the Expert Phase is not mandatory. The DPA may, by majority vote and on its own initiative, commence a proceeding to adopt rules.

- The DPA shall publish its proposal and allow for up to six months of public comment, including comment from the Council. Such comment is to be on the record and made public.
- Should the DPA proceed on its own motion, it shall not adopt a proposal in less than six months absent exigent circumstances.

DPA Enforcement Authority

The DPA should have the authority to prosecute violations of both the authorizing legislation as well as the regulations promulgated pursuant to that statute. This shall include the issuance of injunctions and the levying of fines. The DPA shall have adjudicatory authority, concurrent with federal courts, over alleged violations of its rules brought by third parties.

The DPA should have the authority to prosecute violations of both the authorizing legislation as well as the regulations promulgated pursuant to that statute.

The authorizing legislation should include a private right of action for persons claiming to be damaged by violations of the act. Complainants have the right to elect adjudication either by the federal judiciary or the DPA. Any complaint must be filed within three years of the time of the alleged violation.

Information-Based Government

In the information age, it is more important than ever that federal agencies have access to facts upon which to base a decision. A 2010 U.S. Senate Report accompanying legislation to enhance cyber resiliency stated, "Our government is still organized for the Industrial Age, for assembly lines and mass production. It is a giant, hierarchal conglomerate where the cost of obtaining information and making decisions is high when moving across organizational boundaries. Yet, the Administrative Procedure Act (APA) requires decisions to be made on the facts developed in a proceeding's record.

Unfortunately, the salient facts often are controversial and even elusive. It is not uncommon for advocates to be selective in their presentation of facts in order to manipulate them to their own benefit. Similarly, there has grown up in Washington a cadre of professional commentators and analysts that serve their often-undisclosed corporate sponsors by furthering the selective manipulation of facts.

The DPA requires its own fact-gathering capabilities, including the ability to utilize machine learning and artificial intelligence technology. It would be foolhardy to expect an overseer of the algorithm-driven digital economy to rely on 20th century human-based information gathering and analysis. The tsunami of data-driven actions of the platform companies are unintelligible without the help of machine intelligence. To expect humans to keep pace with algorithm-driven data would be to condemn the DPA to looking at the tsunami through a straw.

The agency's data collection should include the full authority to investigate any entity or activity within its jurisdiction, including the authority to propound interrogatories and to subpoena documents and testimony. The DPA also requires the ability to levy penalties against those who provide inadequate or inaccurate information.