FEDERATED IDENTITY MANAGEMENT AND THE NSTIC: CO-MANAGING INFORMATION PRIVACY

Amanda Craig†

TABLE OF CONTENTS

I. INTRODUCTION

For better or worse, the era of Big Data has arrived.[1] In recent years, more personal information about average consumers has been collected, shared, and used than most of us can fathom, reshaping research in many sectors while intensifying privacy risks.[2] Amidst such vast changes, U.S. privacy law has been stagnant,[3] continuing to enshrine an unworkable system

† JD Candidate, Indiana University Maurer School of Law; MSc, University of Oxford; BS, Northwestern University.

1. *See, e.g.*, VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013).

2. *See, e.g.*, Christine Cignoli, *Big Data Privacy Concerns Spur Research, Innovation*, 2 MOD. INFRASTRUCTURE 12, 12–13 (2013), *available at* http://docs.media.bitpipe.com/io_11x/io_111094/item_727677/Modern%20Infrastructure%20July%202013.pdf ("[Some large] data [collection] projects helped reduce infectious diseases and create a real-time census map of the Ivory Coast—a country where citizens hadn't been counted in years. That data also let researchers see ethnic boundaries, which had long been unclear. . . . Who can argue with curing cancer and encouraging world peace? But analyzing big data can quickly turn into snooping, researchers said. Predicting crimes before they might happen is one example.").

3. Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 249 (2010). Notably, Bamberger and Mulligan argue that, although privacy law "on the books" has been stagnant, their qualitative research indicates that privacy policies "on the ground" have developed considerably since the 1990s. *Id.* at 260.

that relies on individuals exercising their rights to notice and consent.[4] The resiliency of the notice-and-consent approach likely reflects its ability to resolve a relatively recent[5] legal conundrum: privacy is a human right, so the law should protect it,[6] but the importance of privacy is inherently and utterly subjective (and perspectives differ for a variety of rational reasons),[7] so the law risks impinging on individual autonomy without sufficient justification.[8] A notice-and-consent approach resolves this conundrum by focusing on procedural rather than substantive privacy protections.[9] This approach requires that individuals be notified when their data is being collected, informed regarding the way that it will be used, and offered the opportunity to reject or consent to such collection and use.[10] In effect, then, individuals have the right to control or self-manage their own privacy, empowering them to weigh their own interests when deciding whether to access resources and services that may

4. *See, e.g.*, Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent* (Oct. 12, 2009), http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf ("To mitigate privacy threats, it is common to see calls for notice and consent (equivalent to 'informed consent'), which impose a requirement upon actors who collect or use information to explicate their collection and use practices ('give notice') and to allow users an opportunity to choose whether or not to participate ('consent').").

5. Though some scholars trace privacy law to the fourteenth century, many scholars generally agree that, alongside the advancement of information technology, interest in the right to privacy rapidly increased in the 1960s and 1970s. DAVID BANISAR & SIMON DAVIS, GLOBAL INTERNET LIBERTY CAMPAIGN, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND PRACTICE (1998), *available at* http://gilc.org/privacy/survey/intro.html. Indeed, the Fair Information Practice Principles were published by the Organization for Economic Co-operation and Development in 1980 to address growing national concerns related to protecting privacy but maintaining data flows among nations. *See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotection ofprivacyandtransborderflowsofpersonaldata.htm (last visited Feb. 11, 2014) [hereinafter *OECD Guidelines*].

6. Privacy is enshrined as a human right in international law, including in the Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.") and the International Covenant on Civil and Political Rights, art. 15, Dec. 16, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976).

7. *See generally* ALAN F. WESTIN, PRIVACY AND FREEDOM (1967); Alan F. Westin, *Social and Political Dimensions of Privacy*, 59 J. SOC. ISSUES 431, 433–34 (2003) (explaining that individuals have vastly different privacy preferences, which also often change according to context and an individual's condition).

8. Such government intervention would not, of course, represent an anomaly. For instance, the government impinges on individuals' subjective values by rewarding certain behavior with tax incentives; whether such actions are sufficiently justified remains debatable. *See, e.g.*, David T. Ellwood, *The Impact of the Earned Income Tax Credit and Social Policy Reforms on Work, Marriage, and Living Arrangements*, 53 NAT'L TAX J. 1063, 1064 (2000) ("The overall incentive effects are a reflection of taxes, means-tested benefits, work expenses and the like."); Peter J. Wiedenbeck, *Paternalism and Income Tax Reform*, 33 U. KAN. L. REV. 675, 681 (1984) ("But the tax incentive approach is not simply a fiscal shell game if, after full disclosure, voters still prefer selective tax reduction to selective transfer payments."). In effect, the government arguably has acted similarly in the case of privacy, demonstrating the value it perceives in the data revolution by merely requiring notice and consent.

9. *See, e.g.*, STEPHEN HUMPHREYS, INT'L COUNCIL ON HUM. RTS. POL'Y, NAVIGATING THE DATAVERSE: PRIVACY, TECHNOLOGY, HUMAN RIGHTS, at iii (2011), *available at* http://www.ichrp.org/files/reports/64/132_report_en.pdf (explaining that data protection laws focus on "procedural regulation rather than on substantive prohibition").

10. *See, e.g.*, *Privacy Choices for Your Personal Financial Information*, FED. TRADE COMMISSION (Sept. 2012), http://www.consumer.ftc.gov/articles/0222-privacy-choices-your-personal-financial-information (describing privacy notices, consent, and opting out).

intrude upon their privacy.[11]

In the 1980s, when laws reflecting this notice-and-consent approach began to be promulgated,[12] placing a burden on individuals to read and understand privacy policies and to decide whether accessing resources was worth privacy costs was likely more "tolerable."[13] There were far fewer data collectors and users, and personal data was used in more straightforward ways rather than being shared with numerous third parties for developing complex data sets.[14] Still, even early laws reflecting this approach demonstrate the challenges inherent in its implementation. For instance, U.S. laws that require companies to notify and obtain the consent of consumers regarding their data collection and use are often weakened by numerous exceptions.[15] Importantly, though, challenges have escalated significantly in recent years;[16] consumers increasingly rely on online resources, and the scale of our online interactions has dramatically expanded.[17] Assuming that this reliance will not fade and that this scale will not contract, self-management through notice and consent may not be desirable and is not feasible. Information privacy scholar Daniel Solove has explained that the notice-and-consent model is impracticable not only because of cognitive problems but also because of structural problems;[18] "even well-informed and rational individuals cannot appropriately self-manage their privacy."[19]

But developing an alternative approach to protecting privacy may prove just as challenging as continuing to employ the current notice-and-consent model.[20] If privacy choices are not self-managed, then they are at least to some extent managed by another entity, and the alternative of regulating and compelling certain privacy choices on behalf of individuals "risks becoming too paternalistic."[21] For instance, while some consumers may never want to be tracked or to have their data shared, others may always want to be the targets

11. FRED H. CATE, PETER CULLEN & VIKTOR MAYER-SCHÖNBERGER, DATA PROTECTION PRINCIPLES FOR THE 21ST CENTURY: REVISING THE 1980 OECD GUIDELINES 6 (2013).

12. Laws reflecting this approach became the worldwide standard after the development of the Fair Information Practice Principles, which were published by the Organisation for Economic Co-operation and Development in 1980. *OECD Guidelines*, *supra* note 5.

13. CATE, CULLEN & MAYER-SCHÖNBERGER, *supra* note 11, at 6.

14. *Id.*

15. *See, e.g.*, Gramm-Leach-Bliley Financial Modernization Act, Pub. L. 106–102, 113 Stat. 1338 (1999) (containing exceptions in section 502); *see also How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, BUREAU CONSUMER PROTECTION BUS. CENTER (July 2002), http://www.business.ftc.gov/documents/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act (explaining exceptions to the notice and opt-out requirements).

16. *See generally* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 540, 543 (2008) (demonstrating that reading the privacy policies of popular websites would take an individual more than thirty full working days each year), *available at* http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf.

17. *Id.*

18. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880–81 (2013).

19. *Id.* at 1881. For information about cognitive and structural problems inherent in the notice and consent model, see *id.* at 1883–93.

20. *See id.* at 1894–900 (describing alternatives to privacy self-management).

21. *Id.* at 1894.

of relevant marketing, and still others may want targeted ads but only in certain contexts.[22] According to Solove, a more coherent balance among competing interests in supplementing self-management and avoiding excessive paternalism is needed.[23] First, it should be recognized that genuine consent will be nuanced rather than binary,[24] but such nuance must be accounted for without getting too complex to be unworkable.[25] In addition, substantive decisions must be made about the merits of particular forms of data collection and use rather than sustaining notice-and-consent-based neutrality.[26] Such decisions should be codified as basic privacy norms—though again, such codification must not be "overly paternalistic."[27]

Balancing competing interests is a laudable goal, but it is difficult to move beyond the outlines of Solove's "elaborate dance with the tension between self-management and paternalism."[28] What system could achieve more nuanced consent without being overly complex? Or codification of norms that are not overly paternalistic? Moreover, what is *too* complex or paternalistic? These questions will likely have to be answered over time as new systems are adjusted to reflect our capacity for complexity and attitudes toward paternalism in the privacy context.

However, this Essay demonstrates that consumer-focused federated identity management (FIM) may represent a first step toward attempting to achieve Solove's balancing act. For more than a decade, economic dilemmas have plagued consumer-focused FIM, prompting the White House to create the National Strategy for Trusted Identities in Cyberspace (NSTIC),[29] which calls for the development of an "Identity Ecosystem" to simplify user authentication and, in some cases, authorization.[30] According to information privacy scholar Scott David, stakeholders developing this ecosystem should also create a certification or trust mark based on basic privacy norms that are valued in their ecosystem.[31] That certification or mark would then be attached to organizations that earn it, and consumers would be able to rely on those organizations.[32] Notably, the codification of such privacy norms through an industry-recognized certification would be more flexible than doing so through

22. *Consumers Don't Consider Online Tracking to Be Harmless,* MARKETING CHARTS (June 20, 2013), http://www.marketingcharts.com/wp/topics/privacy/consumers-don't-consider-online-tracking-to-be-harmless-30513/.

23. Solove, *supra* note 18, at 1900.

24. A "binary" choice is built into the notice-and-consent model, which assumes that with adequate knowledge about the extent to which online actors are collecting and using information about them, individuals can exercise control by deciding *whether or not* to continue accessing resources associated with such actors.

25. Solove, *supra* note 18, at 1901.

26. *Id.* at 1902–03.

27. *Id.* at 1903.

28. *Id.* at 1900.

29. *See About NSTIC*, NSTIC, http://www.nist.gov/nstic/about-nstic.html (last visited Feb. 11, 2014) (providing background information about NSTIC).

30. *Id.*

31. Telephone Interview with Scott David, Exec. Dir., Law, Tech. & Arts Grp., Univ. of Wash. (Mar. 13, 2013).

32. *Id.*

government regulation. Ultimately, trusted organizations and consumers would "co-manage" the collection and use of consumers' data, creating opportunities for consumers to exercise more nuanced consent.[33] In addition, consumers' data would be better secured by trusted organizations, deepening consumers' privacy protection.[34]

To establish the potential efficacy of consumer-focused FIM projects, this Essay will first provide background information on and examples of FIM. Next, this Essay will describe privacy harms in the digital age and explain the particular significance of power disparities, security, and valuable data flows. Then, it will discuss the NSTIC and the ways in which economic dilemmas that have slowed FIM development in the consumer context may be resolved. Finally, this Essay will demonstrate how the NSTIC could correct power disparities, improve security, and encourage valuable data flows—in other words, how it could execute an "elaborate dance with the tension between self-management and paternalism"[35] while achieving other important privacy goals.

II. FEDERATED IDENTITY MANAGEMENT: BACKGROUND AND EXAMPLES

When individuals email, shop, watch movies, manage finances, or otherwise act online, they interact with service providers (SPs) like Google, Best Buy, Netflix, and Chase Bank. These SPs often associate a unique digital identity with their users.[36] For example, signing into Gmail.com, Netflix.com, and Chase.com requires unique usernames and passwords, which are managed and stored by each SP along with the selected user attributes—like name, age, online habits, or location—that each SP also seeks to record.[37] As a result, users may benefit from mechanisms like narrowly-tailored movie recommendations on Netflix or more secure bank accounts. In addition, managing and tracking unique digital identities often enables SPs to profit by serving targeted ads or otherwise monetizing relevant data.[38]

However, this "multitude of identities" also represents a significant management burden and creates many "potential points of failure."[39] It seems redundant and inefficient to have SPs maintain unique digital identities for each of their customers and to require users to remember usernames and passwords for each of the SPs that they routinely or occasionally access.[40]

---

33. PowerPoint: Scott L. David, "Privacy with Leverage" Engine for Big Data: Summary Description and Legal Requirement Document (Jan. 20, 2013) (on file with author).

34. *Id.*

35. Solove, *supra* note 18, at 1900.

36. Eleanor Birrell & Fred B. Shneider, *Federated Identity Management Systems: A Privacy-Based Characterization*, IEEE SECURITY & PRIVACY, Sept.–Oct. 2013, at 36.

37. *Create Your Google Account*, GOOGLE, https://accounts.google.com/SignUp (last visited Feb. 11, 2014); NETFLIX, https://signup.netflix.com/getstarted?locale=en-US (last visited Feb. 11, 2014); *Enrollment*, CHASE, https://chaseonline.chase.com/public/enroll/IdentifyUser.aspx?LOB=RBGLogon (last visited Feb. 11, 2014).

38. Marshall Brain, *How Internet Cookies Work*, HOWSTUFFWORKS, http://www.howstuffworks.com/cookie.htm (last visited Feb. 11, 2014).

39. Birrell & Shneider, *supra* note 36, at 36.

40. *Id.* at 47.

Security risks are also increased for SPs—from which digital identity information may be stolen—and users, who may be less apt to protect so many scattered digital identities than they would a single digital identity.[41] In addition, individuals' privacy may be at greater risk because their credentials and personal information are in the hands of so many different SPs.

FIM systems attempt to resolve these problems by introducing into the equation "identity providers"[42] (IdPs) that identify and authenticate users on behalf of SPs (and may also aid in the authorization of users on behalf of SPs).[43] An IdP may contract with SPs like Netflix and Chase Bank, and then individuals may be authenticated by that IdP in order to both watch movies and bank. Though critics cite serious security and privacy concerns,[44] ideally, everyone benefits through this system: individuals only have to log in and share their credentials with one entity to access multiple websites; SPs delegate account management tasks (such as password resets) and worry less about losing customer information in the event of data theft; and IdPs are able to focus on improving identification, authentication, and authorization methods.[45]

But the varied success rates of FIM projects,[46] which have been developing since the late 1990s, suggest that everyone does not always benefit

41. *See* Shirley Radack, *Managing Identity Requirements for Remote Users of Information Systems to Protect System Security and Information Privacy*, ITL BULL. (U.S. Dep't of Commerce), Jan. 2013, at 1, *available at* http://csrc.nist.gov/publications/nistbul/itlbul2013_01.pdf (noting that some threats to security include "eavesdropping and stealing of usernames and identity credentials; redirection of users to fraudulent websites; man-in-the-middle attacks that intercept and alter authentication messages; and takeover of authenticated sessions.").

42. Birrell & Shneider, *supra* note 36, at 36.

43. Identity management occurs both offline and online and involves the processes of: (1) identifying a person (identification); (2) verifying that a particular person is that previously identified person (authentication); and (3) determining what rights and privileges should be accorded to the identified person (authorization). When obtaining a driver's license (as an example of an offline system), an individual must bring his or her social security card and a few pieces of mail to verify identity and residence, and later, that individual will use his or her driver's license to authenticate or verify his or her identity. Then, that individual may use his or her driver's license to prove that he or she has the right or is "authorized" to drive or to drink alcohol. *See generally* Thomas J. Smedinghoff, Federated Identity Management: Balancing Privacy Rights, Liability Risks, and the Duty to Authenticate (Aug. 21, 2009) (unpublished manuscript), *available at* http://ssrn.com/abstract=1471599. Notably, while single sign-on, a popular form of FIM, allows user authentication, other FIM systems will, using the same user attributes, allow for both IdPs to authenticate users *and* SPs to authorize those users' access to certain internal resources. *See, e.g.*, David W. Chadwick & George Inman, *Attribute Aggregation in Federated Identity Management*, COMPUTER, May 2009, at 33, 33–40 (describing how in CardSpace and Shibboleth systems SPs rely on IdPs to "authenticate the users and provide their identity attributes"). *But see* Jean Camp, *Identity Management's Misaligned Incentives*, SECURITY & PRIVACY, Nov.–Dec. 2010, at 90, 90 (arguing that NSTIC confuses "identity" with authentication and authorization).

44. *See, e.g.*, Camp, *supra* note 43, at 90 (arguing that FIM will not resolve already misaligned incentives for protecting identity, including our use of identity credentials for accessing both low- and high-value data—which results in low-value collectors not having incentives to spend significant resources to protect credentials and high-value collectors not having significant incentives to protect credentials that may be exploited more easily elsewhere); *see also* Eve Maler & Drummond Reed, *The Venn of Identity: Options and Issues in Federated Identity Management*, IEEE SECURITY & PRIVACY, Mar.–Apr. 2008, at 16, 16–23 (describing new security and privacy risks that FIM provokes).

45. Maler & Reed, *supra* note 44, at 17.

46. Due to the limited scope of this Essay, only a few FIM projects are discussed. For information about additional projects, see Birrell & Shneider, *supra* note 36; Susan Landau & Tyler Moore, *Economic Tussles in Federated Identity Management*, FIRST MONDAY (Oct. 1, 2012), http://journals.uic.edu/ojs/index.php/fm/article/view/4254/3340.

equally. Successful FIM projects have largely been in the enterprise-to-enterprise context. In particular, sector-specific and inter-industry projects like SAFE BioPharma, which was first developed because doctors needed a secure way to submit clinical trial data,[47] and Certipath,[48] which is used by aerospace defense contractors and the U.S. government, have been successful. The only consumer-focused FIM system that has been successful is Facebook Connect, a single sign-on system in which users access additional SPs—like news websites—by logging on to Facebook.[49] However, InCommon, a subsidiary of Internet2, has built a successful federation known as Shibboleth to benefit students, professors, and researchers. As of 2011, 189 universities were functioning as IdPs,[50] while libraries and nonprofit or commercial information providers like JSTOR or LexisNexis function as SPs.[51] Less successful FIM projects and stakeholder incentive problems, which help to explain the variations in FIM project success rates, will be discussed below in Part IV.

III. CONCEPTUALIZING PRIVACY HARMS IN THE DIGITAL AGE

Despite the general lack of success of consumer-focused FIM projects, one of the goals of FIM is protecting the information privacy of individuals. The idea is that, if users share their credentials with fewer SPs, then their personal information will be less scattered and their privacy better protected.[52] But do users even want this privacy protection? This Part considers privacy harms in the digital age with the ultimate goal of determining the extent to which FIM projects address important privacy harms and associated policy issues.

Although privacy is sometimes described as a human right, characterizing privacy harms is a notoriously difficult endeavor.[53] While financial harms resulting from incidents like identity theft and physical harms resulting from incidents like stalking are reasonably quantifiable, such financial and physical harms may be remedied by legal protections outside of privacy law.[54] Other, unprotected types of harms—like non-defamatory reputational harm resulting in anything from embarrassment to severe emotional distress—are much more difficult to quantify because they are so contextual. As Solove has written, "many privacy violations are akin to a bee sting."[55] Yet to those who are allergic to bee stings—or particularly sensitive to certain privacy violations—such events are catastrophic. In other words, privacy harm is extremely

47. Telephone Interview with Tom Smedinghoff, Partner, Edwards Wildman Palmer LLP (Mar. 12, 2013).

48. *About*, CertiPath, https://www.certipath.com/about (last visited Feb. 11, 2014).

49. Landau & Moore, *supra* note 46, at 16.

50. *Id.* at 32.

51. *Id.* at 16.

52. Susan Landau et al., *Achieving Privacy in a Federated Identity Management System*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY 51−70 (Roger Dingledine & Philippe Golle eds., 2009).

53. *See, e.g.*, BANISAR & DAVIS, *supra* note 5.

54. *See, e.g.*, 18 U.S.C. § 1028 (2012) (noting that "[f]raud related to activity in connection with identification documents, authentication features, and information" is a federal crime).

55. Solove, *supra* note 18, at 1891.

relative.

Another difficulty with quantifying privacy harms is that small, abstract privacy harms aggregate over time; people may agree to many forms of data collection and use because harmful effects only emerge from later, secondary and combined uses of their data.[56] Again, according to Solove, "[o]ne bee sting can be shrugged off, but a hundred or a thousand can be lethal."[57] In addition, privacy harms may be dispersed among individuals, none of whom experiences severe enough harm to take legal action. For instance, if a company steals one cent from everyone, the harm to each of us is minimal and hardly seems worth our time or energy, but the law should surely still recognize the aggregate harm.[58] This unique nature of privacy harm helps to explain why our liberal assumptions about the power of notice and consent, or self-managing approaches to information privacy, are unworkable. It seems intuitive that individuals should determine for themselves when and how information about them is communicated to others unless they cannot fully evaluate the harm to themselves or to their societies.

Once privacy harms are viewed in aggregate on the societal level, characterizing them is more straightforward. Most significantly, lack of information privacy may have a chilling effect on society. If individuals do not have a "zone of informational autonomy,"[59] then their creativity and intellectual growth may be stunted, which will in turn stunt our cultural development.[60] Put less abstractly, if individuals fear that their personal information space may be breached by a security incident or aggregated and shared in a way that damages them, then they may be hesitant to take risks that will benefit society. This broader social importance of privacy is embedded in Neil Richards's concept of "intellectual privacy," which is "the ability, whether protected by law or social circumstance, to develop ideas and beliefs away from the unwanted gaze or interference of others."[61] According to Richards, intellectual privacy is so foundational to our democratic culture that it should be guarded from both public and private actors.[62]

Notably, highlighting this societal harm is not intended to render information privacy harms that occur at the individual level meaningless. Rather, recognizing this harm is intended to emphasize the link between the difficulty of characterizing such harms at the individual level and the hands-off, highly personal approach of notice and consent, which ignores larger social values. This tension between social harms and individual harms is also reflected in Solove's balancing of his interests in supplementing information privacy self-management and avoiding excessive paternalism in doing so.[63] As

56. *Id.*
57. *Id.*
58. *Id.* at 1889.
59. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1428 (2000).
60. Solove, *supra* note 18, at 1892.
61. Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 389 (2008).
62. *Id.* at 429.
63. Solove, *supra* note 18, at 1894.

such, this Part demonstrates that larger social values must be brought into the fold if effective balancing is to be undertaken.

Recognizing privacy harms through an aggregate lens is also essential to understanding which among the many possible problems associated with privacy harms deserves most attention. This Essay argues that the three most important policy issues are power disparities, security, and valuable data flows, which are all visible at the societal level. Power disparities between consumers and online actors that collect and use data about them are vastly out of balance. This is reflected in the binary way in which notice-and-consent has developed; consumers often must choose between sharing their data and accessing a wanted (or even needed) service or not sharing their data and not accessing that service. In other words, consumers have no bargaining power, and their choices seem to be structured in ways that nearly force them to consent.[64] If power disparities are not corrected, individuals may continue to feel that their information privacy cannot be protected, and the above-described chilling effect on society may result. In addition, if individuals are not confident that the security of their personal information is protected, then they may not be able to rely on society's information systems, and a chilling effect may also result. Lastly, if valuable data flows are not sustained, then cultural development may similarly be stunted.[65]

IV. THE NSTIC AND TRUST FRAMEWORKS: CHANGING THE PRIVACY EQUATION?

If the most important information privacy harms-related policy issues are correcting power disparities, ensuring security, and sustaining valuable data flows, then to what extent are these issues being addressed by current policy proposals? The next three Parts of this Essay will argue that FIM projects have the potential to effectively address these issues with the help of the NSTIC. This Part will first provide background information on the development and structure of the NSTIC.

In April 2011, the White House released its final version of the NSTIC,[66] which was an outgrowth of President Obama's 2009 Cyberspace Policy Review.[67] Government agencies, business leaders, and privacy advocates collaborated on the NSTIC drafts,[68] but, according to the final version, the

64. *Id.* at 1898.

65. *See, e.g.*, CATE, CULLEN & MAYER-SCHÖNBERGER, *supra* note 11; MAYER-SCHÖNBERGER & CUKIER, *supra* note 1 (demonstrating and describing the importance of valuable data flows for advancements in many areas of research, including medicine, education, and transportation); *OECD Guidelines*, *supra* note 5.

66. Elizabeth Montalbano, *White House Issues Online Trusted Identities Plan*, INFORMATIONWEEK (Apr. 15, 2011, 2:48 PM), http://www.informationweek.com/government/security/white-houses-issues-online-trusted-ident/229401701.

67. The Review's "Near-Term Action Plan" calls for building "a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests." DEP'T OF HOMELAND SEC., CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 37 (2009).

68. Howard A. Schmidt, *The National Strategy for Trusted Identities in Cyberspace*, WHITE HOUSE BLOG (June 25, 2010, 2:00 PM), http://www.whitehouse.gov/blog/2010/06/25/national-strategy-trusted-

private sector should lead while the government acts as a facilitator.[69] Within the Department of Commerce, the National Institute of Standards and Technology (NIST) and its newly established National Program Office coordinate federal government activities to implement the NSTIC and act as a focal point between the public and private sectors.[70]

According to Scott David and Tom Smedinghoff, an information privacy practitioner, the NSTIC represents the White House's frustration with the lack of consumer-focused FIM projects as well as recognition that the structural challenges to such projects are significant.[71] As such, the NSTIC is intended to develop possible resolutions to those challenges. More specifically, the NSTIC intends to establish an "Identity Ecosystem" so that individuals can "validate their identities securely when they're doing sensitive transactions."[72] This Ecosystem will protect the privacy of individuals by reducing their need "to share personally identifiable information (PII) at multiple websites and by establishing consistent policies about how organizations use and manage PII."[73]

To accomplish these goals, the NSTIC includes two parts: (1) an Identity Ecosystem Steering Group (IDESG); and (2) pilot projects.[74] There have been two rounds of pilot grants, which are funded by the NIST.[75] In 2012, the first round awarded more than $9 million to five different proposals.[76] Last September, the 2013 grants awarded over $7 million to five different proposals[77] (similar to the 2012 grants) and over $2 million to the states of Pennsylvania and Michigan, which will "test new online identity technologies to improve access to government services and the delivery of federal assistance programs."[78] In January 2014, the NIST held an Applicants' Conference for 2014 grant applicants.[79]

The pilot projects represent "very different worldviews," according to Ken Klingenstein, who directs the Internet2 Middleware and Security Initiatives and is involved in the University Corporation for Advanced Internet Development (UCAID) project, which received a pilot grant in 2012.[80] For

identities-cyberspace.

69. Montalbano, *supra* note 66.

70. *About NSTIC*, *supra* note 29.

71. Telephone Interview with Scott David, *supra* note 31; Telephone Interview with Tom Smedinghoff, *supra* note 47.

72. *About NSTIC*, *supra* note 29.

73. *Id.*

74. *Nat'l Strategy for Trusted Identities in Cyberspace*, NAT'L INST. STANDARDS & TECH., http://www.nist.gov/nstic/index.html (last visited Feb. 11, 2014).

75. *Pilot Projects*, NAT'L INST. STANDARDS & TECH., http://www.nist.gov/nstic/pilot-projects.html (last visited Feb. 11, 2014).

76. *2012 Pilot Projects*, NAT'L INST. STANDARDS & TECH., http://www.nist.gov/nstic/pilot-projects2012.html (last visited Feb. 11, 2014).

77. *NIST Awards Grants to Improve Online Security and Privacy*, NAT'L INST. STANDARDS & TECH. (Sept. 17, 2013), http://www.nist.gov/itl/nstic-091713.cfm [hereinafter *NIST Awards*].

78. *Grants to Two States Will Support Improved Access to Services and Reduce Fraud*, NAT'L INST. STANDARDS & TECH. (Sept. 23, 2013), http://www.nist.gov/itl/nstic-092313.cfm.

79. *2014 Pilot Projects*, NAT'L INST. STANDARDS & TECH., http://www.nist.gov/nstic/pilot-projects.html (last visited Feb. 11, 2014).

80. Telephone Interview with Ken Klingenstein, Dir., Internet2 Middleware & Sec. Initiative (Mar. 4,

instance, the American Association of Motor Vehicle Administrators project[81] is attempting to build an infrastructure that many other FIM projects would be able to use, whereas others are taking narrower approaches.[82] The Criterion Systems project, through which consumers may selectively share shopping and other preferences to both reduce fraud and enhance their user experience,[83] is trying to determine whether there is a marketplace for the selling of verified attributes.[84] Meanwhile, UCAID, which is also known as the Internet2 project, is attempting to develop "citizen" attributes that can be applied beyond the university context.[85] According to Smedinghoff, the experimentation represented in these diverse pilot projects represents an important opportunity for the private sector to develop viable business models that avoid economic dilemmas, which have thus far hindered the creation of FIM projects.[86]

To balance the ad-hoc experimentation of the pilot projects, the IDESG was created to develop and adopt policies and standards for the Identity Ecosystem Framework.[87] Any individual or organization interested in the development of the Identity Ecosystem can participate in the IDESG, which is a private sector-led group.[88] Within the IDESG, individuals and groups may join various standing committees and working groups, which elect their own leaders, draft their own charters, and organize their own work.[89] For instance, in March 2013, the Privacy Subcommittee used its newly developed "privacy evaluation methodology" (PEM) to simultaneously test the IDESG website and demonstrate the PEM's utility.[90]

According to Scott David, the IDESG should be developing standards that it could use to create a certification or "trust" mark that identity providers could earn through compliance with its standards.[91] In June 2013, an IDESG committee entitled the "Trust Frameworks and Trustmark Committee" (TFTM Committee) adopted its charter and was officially established.[92] The charter states that one of the committee's goals is to develop and manage a "trustmark program," which would certify entities that adopt and implement the NSTIC's

---

2013).

81. For more information, see *2012 Pilot Projects*, *supra* note 76.

82. Telephone Interview with Ken Klingenstein, *supra* note 80.

83. For more information, see *2012 Pilot Projects*, *supra* note 76.

84. Telephone Interview with Ken Klingenstein, *supra* note 80.

85. For more information on the Internet2 pilot, see Steve Olshansky, *Scalable Privacy: An NSTIC Pilot for the Identity Ecosystem*, INTERNET2 (Nov. 27, 2013), https://spaces.internet2.edu/display/scalepriv/Scalable+Privacy.

86. Telephone Interview with Tom Smedinghoff, *supra* note 47.

87. IDENTITY ECOSYSTEM STEERING GRP., RULES OF ASSOCIATION OF THE IDENTITY ECOSYSTEM STEERING GROUP 7 (2013), *available at* https://www.idecosystem.org/roa.

88. *Id.* at 11.

89. *Id.* at 12.

90. Stephen Wilson, Preliminary Privacy Evaluation: IDESG Website (Mar. 2013) (unpublished report) (on file with author). Individuals may sign up to receive information about Privacy Coordination Committee activities and similar reports at http://mail.idecosystem.org/mailman/listinfo/privacy_sc_idecosystem.org.

91. Telephone Interview with Scott David, *supra* note 31.

92. *Charter of the Trust Frameworks and Trustmark Committee*, IDENTITY ECOSYSTEM STEERING GRP. (June 14, 2013), http://www.idecosystem.org/group/trust-framework-and-trustmark-committee (follow "Trust Framework & Trustmark Committee Charter" hyperlink) (last visited Feb. 11, 2014).

guiding principles.[93] According to the TFTM Committee's recent meeting minutes, which are publicly available, discussions regarding the form and function of a trust mark or certification are ongoing.[94] In addition, one of the recipients of the 2013 pilot grants, Georgia Tech Research Corporation, designed a project that will attempt to develop and demonstrate a "Trustmark Framework."[95]

An IDESG or pilot-project developed certification or trust mark could function like a Good Housekeeping seal, on which service providers and individual consumers could rely. The concept of using such a trust mark is not unprecedented on the Internet; the Better Business Bureau (BBB) has developed a Code of Business Practices that companies must abide by to earn its accreditation.[96] The code is composed of eight principles, one of which encourages businesses to "safeguard privacy," which it defines as protecting data against mishandling or fraud, collecting personal information only as needed, and respecting the preferences of customers regarding the use of their information.[97] The benefit of the IDESG or an NSTIC pilot program developing a certification or trust mark in the FIM context and the different approach that the IDESG should take from the BBB are described in Part VI of this Essay.

V. RESOLVING THE FIM STAKEHOLDER INCENTIVES PROBLEM

Before discussing the development and value of an IDESG-sponsored trust mark, this Essay must discuss how the NSTIC may resolve FIM stakeholder incentives problems because if it cannot do so, then the NSTIC will not be successful, and the development of such a mark may be irrelevant. As was noted in Part II of this Essay, outside of the enterprise-to-enterprise and particularly the inter-industry contexts, adoption of FIM systems has largely been unsuccessful. Disputes over the assignment of liability for authentication failures and privacy or security breaches are often cited as reasons for slow adoption.[98] Systems could become unavailable to authenticate users, causing problems for service providers relying on their operation, or "authentication itself could fail, and unauthorized users could be incorrectly authenticated as other users."[99] In any case, when something goes wrong, a recurrent question arises: who should pay for such failures and breaches—individuals, IdPs, or SPs?

While Susan Landau and Tyler Moore acknowledge these liability

93. *Id.*

94. Trust Framework and Trust Mark Committee: Meeting Minutes, IDENTITY ECOSYSTEM STEERING GRP. (Jan. 29, 2014), https://www.idecosystem.org/filedepot?cid=72&fid=1100 (last visited Feb. 11, 2014).

95. *NIST Awards*, *supra* note 77.

96. *BBB Code of Business Practices (BBB Accreditation Standards)*, COUNCIL BETTER BUS. BUREAUS, http://www.bbb.org/council/for-businesses/about-bbb-accreditation/bbb-code-of-business-practices-bbb-accreditation-standards/ (last updated Jan. 1, 2009).

97. *Id.*

98. Landau & Moore, *supra* note 46.

99. *Id.*

problems, both believe that they are actually just one piece of a larger problem, the root of which lies at the nexus of a "complex tangle" of adoption-slowing economic issues.[100] More specifically, FIM systems present a classic case of "economic tussle" because economic benefits often do not accrue to all engaged or relevant parties.[101] As such, Landau and Moore argue, while FIM systems that benefit IdPs, SPs, and users have been successful, those that largely benefit just one or two of the engaged or relevant parties have failed; in such cases, IdPs or SPs in particular have not had sufficient incentives to undertake the expense of adopting a new system.[102]

Landau and Moore highlight four economic "tussles," which occur whenever stakeholder incentives conflict.[103] First, who gets to collect transactional data—including personal information and behavioral choices—that results from interactions with users?[104] Transactional data is incredibly valuable in our Big Data world, so which stakeholder gets access to and controls such data is crucial, especially for companies that rely on it for targeted advertisements.[105] In addition, even in industrial contexts, some companies may prefer to continue collecting transactional data, which they use to conduct audits and discover misuse of system resources.[106]

Second, Landau and Moore ask: Who sets the rules of authentication?[107] When it is unclear which parties should serve as IdPs and which should serve as SPs, both parties may compete to be the IdP and to determine the system's "rules," upsetting the difficult balancing work involved in setting authentication requirements.[108] No standard, or set of rules, dominates among federated identity technologies,[109] and the costs of interoperating with complex information technology systems that follow different rules are high.[110] Moreover, as Ross Anderson demonstrates, companies may be concerned about who sets the rules of authentication because their adoption may not necessarily reflect the most secure engineering.[111] In describing how 3D Secure (i.e., Verified by VISA) has become one of the most widely adopted FIM systems in the world, Anderson highlights how "strong adoption incentives" have trumped "bad engineering."[112]

---

100. *Id.*
101. *Id.*
102. *Id.*
103. *Id.*
104. *Id.*
105. *Id.*
106. Jostein Jensen & Martin Giljie Jaatun, *Federated Identity Management—We Built It; Why Won't They Come?*, IEEE SECURITY & PRIVACY, Mar.–Apr. 2013, at 34, 35–36.
107. Landau & Moore, *supra* note 46.
108. *Id.*
109. *See* Maler & Reed, *supra* note 44, at 22 ("Interoperability is an ongoing challenge for federated identity. Even within a single protocol, interoperability among online partners can be difficult because of protocol options, conformance variations, and the architecture's cross-platform nature.").
110. Jensen & Jaatun, *supra* note 106, at 37–38.
111. Ross Anderson, *Can We Fix the Security Economics of Federated Authentication*, *in* SECURITY PROTOCOLS XIX 25, 26–27 (B. Christianson et al. eds., 2011).
112. *Id.*

Landau and Moore thirdly ask: What happens when things go wrong?[113] Without clear legal rules or mutual interest in success based on existing business relationships (which may explain the success of Shibboleth, in which the roles of IdPs and SPs are "symmetrical" and Internet2 is able to leverage its existing connections with universities), assignment of liability is critical.[114] Relatedly, assigning responsibility for revoking access of unintended or malicious users and reinstating access of intended users is likely critical to both IdPs and SPs adopting an FIM system. Anderson asks who should be responsible for these actions in the event that a smart phone that acts as a "mobile wallet"—which would hold, for example, credit cards, loyalty cards, gift cards, and your driver's license—is lost or stolen.[115] As above, incentives to cooperate are of chief importance.[116] He argues that an individual's chosen "default" credit card should be responsible for revocation (as an award to the consumer for choosing it to be the "default" card), and an individual's phone company should be responsible for reinstating access.[117] If the phone company is able to sell to its former customer a new phone with the required access immediately enabled while its competitors can only sell those same customers a new phone with some minimum hassle and a few days of access delay, then it should be incentivized to do so.[118]

Fourth and finally, in analyzing FIM economic tussles, Landau and Moore ask: Who gains and who loses from interoperability?[119] They write that users likely benefit from being authenticated by one IdP to access multiple SPs, but the benefits and risks of increasing interoperability vary by application and stakeholder.[120] For instance, IdPs may value interoperability because it means that they will acquire more data from customers, but SPs may not value interoperability if it means that they will acquire fewer new customers.[121] Similarly, industrial companies that offer a relatively limited set of services to a limited number of external users may find the costs of implementing FIM high and any offsetting advantages insufficient.[122] Their adoption of such management systems would likely depend, then, on contractual obligations to comply with the policies of companies that are more motivated to adopt FIM approaches and are within their supply chain.[123]

In short, stakeholder interests are divergent. Users have convenience, their digital identity, and privacy preferences at stake. Economically motivated IdPs are likely most concerned with increasing user and SP confidence in their ability to protect credentials, limiting liability risks, and

113. Landau & Moore, *supra* note 46.
114. *Id.*
115. Anderson, *supra* note 111, at 27–29.
116. *Id.* at 31.
117. *Id.* at 30.
118. *Id.*
119. Landau & Moore, *supra* note 46.
120. *Id.*
121. *Id.*
122. Jensen & Jaatun, *supra* note 106, at 39.
123. *Id.*

controlling data that they can monetize. Economically motivated SPs are likely most concerned with ensuring constant access to their services, limiting liability risks, and continuing to gather data that they can monetize.

The effect of attempting to merge these divergent interests is conspicuous in failed FIM projects.[124] For example, OpenID Connect is an FIM system that repurposed Shibboleth's FIM technology in the commercial setting.[125] It was established in 2005 as a nonprofit platform that enabled single sign-on for Internet services.[126] While OpenID has recruited many IdPs, very few SPs have signed up because the benefits to SPs are "much less obvious,"[127] and there has been a lack of demand from users.[128] According to Landau and Moore, most IdPs have also done little to encourage adoption.[129] Knowing that many Web services depend on targeted advertising, for which demographic information is essential, OpenID has developed an "attribute exchange mechanism," which would allow IdPs and SPs to exchange users' demographic information.[130] IdPs are "free to choose" which user demographic information to share, but to date, most IdPs have "elected to share very few user details" with SPs.[131] Meanwhile, OpenID incentivizes user loyalty to IdPs, which learn about their user's browsing habits and apply that information toward creating more tailored user profiles to target in their advertising.[132]

How might this problem of divergent interests be resolved? Anderson proposes the above-described model in the mobile wallet context.[133] Landau and Moore do not explicitly propose a solution, but their paper references the importance of federal government regulation.[134] For example, they explain that the medical billing system of Aetna, an insurance company, is federated. Medical billing offices act as SPs, and Aetna and NaviMedix, a provider of software for secure online systems, serve as IdPs.[135] Notably, Aetna and NaviMedix use NIST authentication guidelines to coordinate levels of credentialing assurance, which Landau and Moore describe as crucial to this system's success; the use of these guidelines also demonstrates the authority that a trust mark developed by a NIST-associated group like the IDESG or a pilot project may possess.[136] Landau and Moore also attribute the success of Aetna and NaviMedix to the Health Insurance Portability and Accountability Act (HIPPA), which clarified the responsibilities of organizations within the system to protect the privacy of patient information and created liability for

124. OPENID, http://openid.net/connect/ (last visited Feb. 11, 2014).
125. *Id.*
126. Landau & Moore, *supra* note 46.
127. *Id.*
128. Anderson, *supra* note 111, at 27.
129. Landau & Moore, *supra* note 46.
130. *Id.*
131. *Id.*
132. *Id.*
133. Anderson, *supra* note 111, at 3–8.
134. Landau & Moore, *supra* note 46.
135. *Id.*
136. *Id.*

failing to do so.[137]

However, the risk in relying on federal regulation to clarify liability or create rules about information privacy is that the government will get it wrong and bring the already slow development of FIM projects to a halt. The government should proceed with caution, according to Tom Smedinghoff, who analogizes FIM with the invention of automobiles in the early 1900s.[138] At that point, the government could have stopped innovation by creating investor risk-laden rules about how cars should be built to ensure safety. Instead, the government facilitated further development by building roads, developing gas standards, and figuring out how to control intersections. Similarly, Smedinghoff argues, FIM is not yet a viable business, so over-regulating it may drive investors and innovation away.[139] But how might the government facilitate the development of FIM? One option might be to create rules about tangential issues like "de-identified data"—as it did about tangential issues like gas in the early twentieth century.

Creating such rules would support the data system structure being proposed by Scott David and scholars from the Massachusetts Institute of Technology (MIT).[140] They use a banking model to analogize an approach to FIM, focusing on three types of banking services.[141] At level one, banks serve as safe deposit boxes, "locking down" received assets as a service performed for customers.[142] Similarly, in the FIM context, IdPs would protect customers' personal information as received assets.[143] At level two, banks provide fiduciary or trust-based services, transferring received assets—also as a service performed for customers.[144] In the FIM context, this is analogized as IdPs transferring authentication and authorization credentials to SPs.[145] Finally, at level three, banks provide interest-bearing checking or savings accounts.[146] They transfer assets as principal (on their own rather than on a customer's behalf) and earn revenue, a portion of which is shared with customers as "interest."[147] Likewise, in the FIM context, IdPs could circulate or sell de-identified data or data of which customers contractually approve.[148] A portion of the profits earned by selling such data could then be used to create an insurance pool that would cover IdP liability in the case of failed authentication or a security breach.[149]

This Essay advocates for the adoption of David's and MIT's data system structure because it could effectively address not only the problem of divergent

137. *Id.*
138. Telephone Interview with Tom Smedinghoff, *supra* note 47.
139. *Id.*
140. David, *supra* note 33.
141. *Id.*
142. *Id.*
143. *Id.*
144. *Id.*
145. *Id.*
146. *Id.*
147. *Id.*
148. *Id.*
149. *Id.*

stakeholder interests identified by Landau and Moore but also the three important policy issues identified above. The next Part returns to these issues and explains how the NSTIC and this data system structure complement each other and impact societal privacy harms.

VI. NSTIC CERIFICATION AND DAVID'S DATA SYSTEM: ANALYZING PRIVACY POLICY ISSUES

This Part evaluates an entirely speculative prompt: if the IDESG develops a certification or trust mark that is widely adopted, and FIM projects resembling Scott David's banking-like data system structure develop, then how will privacy harms and important policy issues tied to such harms be impacted? Such speculation is valuable to the extent that it demonstrates these systems' potential to correct harms and address policy issues, encouraging and directing investment in a space in which, according to the NIST's 2014 budget proposals, investment is currently increasing.[150] To that end, this Part evaluates the extent to which the adoption of an IDESG trust mark and David's banking-like data system structure may correct power disparities, improve security, and encourage valuable data flows.

As was articulated above, in our world of Big Data, consumers do not benefit from an information privacy system that provides rights to notice and consent only.[151] Instead, our system of notice and consent has created enormous power disparities between individuals, who are obliged to consent, and online actors that are in effect given a constant green light to collect and use individuals' data as they desire.[152] Employed together, an IDESG certification or trust mark and David's data system may correct these power disparities.[153] First, since they often do not have the required time or information to evaluate privacy policies, individuals will instead be able to rely on a trust mark.[154] In this way, they will be able to exercise power by choosing to form contractual relationships only with IdPs that have gained such certification.

Second, individuals will be empowered through the "co-managed use" of their data as required by David's data system.[155] Without this system, it is foreseeable that FIM projects may develop in a way in which economics demand that user data be passed from IdPs to SPs without a significant role for individuals to play.[156] But in David's system, individuals and IdPs are interdependent.[157] Individuals need IdPs that can secure their credentials in a

150. Powerpoint: Patrick Gallagher, NIST FY 2014 Budget Overview: Working with Industry to Accelerate Innovation (Apr. 16, 2013), *available at* http://www.nist.gov/director/ocla/upload/UPDATED-FY2014_Congressional_Budget_Rollout_Presentationv7-4-16-13.pdf.

151. *See* Barocas & Nissenbaum, *supra* note 4 (discussing how notice and consent rights alone are not beneficial to consumers).

152. *Id.*

153. David, *supra* note 33.

154. *Id.*

155. *Id.*

156. *Id.*

157. *Id.*

safe deposit box as well as transfer their credentials as a fiduciary or trust-based service.[158] In turn, IdPs need to acquire individuals' personal information as assets and to form contractual agreements with individuals regarding what data they can transfer as principal.[159] Most significantly, this system enables consumers to make more informed and more nuanced choices about how their personal information is used while retaining the right to expose their data to additional uses if they individually prefer to do so.[160]

However, it is still possible that power disparities will remain if these systems are adopted. For example, the interdependence of IdPs and individuals is at least partially dependent on individuals' engagement with contractual opportunities related to their privacy rights.[161] IdPs can sell personal information to SPs, and individuals need sufficient knowledge to exercise choice.[162] Currently, individuals do not engage with online contracts; they click through privacy policies and consent to them without even reading them.[163] Still, these systems encourage more engaged consumer behavior because it is much more reasonable for a consumer to undertake contractual bargaining with one IdP than with many SPs.

As extensions of the FIM system, an IDESG trust mark and David's data system may also positively impact online security.[164] Data privacy cannot be achieved without data security, and many consumers' chief privacy concerns are actually related to concerns about data breaches involving their personal information.[165] FIM systems in general may substantially improve the protection of such information.[166] First, IdPs are able to specialize in authentication, so they should divert more resources to developing and implementing better technology than SPs currently do.[167] Second, individuals should also be more willing to devote more resources—like time—to ensuring that their credentials are well-protected when they are managing such credentials with one IdP rather than with many SPs.[168] For instance, they may be more willing to maintain complicated, regularly changed passwords or to use multi-factor authentication.[169] According to Klingenstein, multi-factor authentication is one of the most powerful security measures that could be implemented, and Internet2's 2012 pilot is focused on signing up as many

158. *Id.*
159. *Id.*
160. *Id.*
161. *Id.*
162. *Id.*
163. CATE, CULLEN & MAYER-SCHÖNBERGER, *supra* note 11, at 6–7.
164. David, *supra* note 33.
165. *See Consumer Privacy: Data Security/Breach*, CTR. FOR DEMOCRACY & TECH., https://www.cdt.org/issue/data-securitybreach (last visited Feb. 14, 2014) ("Consumers are concerned that they lack control over the personal information, and identity theft has become all too frequent.").
166. *See* Smedinghoff, *supra* note 43, at 2 (describing how FIM could reduce the burden placed on consumers and service providers by outsourcing identity management to a third party).
167. *1.2.1 Identity Provider Deployment*, ORACLE, http://docs.oracle.com/cd/E19575-01/820-5986/ghmrq/index.html (last visited Feb. 10, 2014).
168. *See* Landau & Moore, *supra* note 46, at 17 (explaining the ease of access and privacy benefits to users).
169. *Id.*

universities as possible to deploy the technology in ways that they envision being most effective.[170]

However, as with power disparities, FIM systems do not ensure improved security.[171] Because IdPs would have centralized control over users' personal information, FIM systems create new risks;[172] hackers may be much more motivated to breach an IdP that possesses so much diverse personal information than they are to breach SPs with an unknown quantity of such information.[173] In addition, as above, the adoption of improved passwords and multi-factor authentication may be dependent on the will of individuals (unless organizations mandate these technological changes). Adopting these technologies is much more manageable when individuals are only using them to interact with one IdP rather than with many SPs, but doing so will still require some consumer effort.

Finally, an IDESG trust mark and David's data system may sustain valuable data flows, which will continue to be an important policy issue in the future.[174] Our society is increasingly dependent on data flows in many sectors, including the health and financial sectors, and as our reliance on data expands (and is likely further accentuated by new technologies), the importance of these flows will similarly intensify.[175] IDESG and David's system may contribute by creating systems to support and enable the flow of de-identified data, potentially standardized through a trust mark, government regulation, or revised Fair Information Practice Principles.[176] Ideally, such standardized de-identified data will flow seamlessly among jurisdictions.

However, there will likely be unforeseen challenges to sustaining valuable data flows until FIM systems are globalized.[177] FIM systems' reliance on certain attributes may prove problematic because the preferred types and structures of attributes will likely vary across jurisdictions.[178] For instance, according to Klingenstein, long Spanish surnames resulted in a temporary disruption to an attribute system that did not allow enough spaces for such names.[179] More complicated or values-related differences among jurisdictions will likely create more than a temporary disruption.[180] In addition, FIM projects are being developed internationally.[181] If such projects

170. Telephone Interview with Ken Klingenstein, *supra* note 80.

171. *See* Smedinghoff, *supra* note 43, at 15–23 (describing all the risks associated with use of federated identity management).

172. *Id.*

173. *Id.*

174. CATE, CULLEN & MAYER- SCHÖNBERGER, *supra* note 11, at 9.

175. *See* Solove, *supra* note 18, at 1895 (describing the societal trend of providing and sharing more data online).

176. Telephone Interview with Scott David, *supra* note 31.

177. *See OECD Guidelines*, *supra* note 5 (discussing the inherent difficulties in easing data flows through different countries).

178. Jennifer Barrigar, *Guided Literature Review: Identity Management Systems*, OFF. PRIVACY COMMISSIONER CAN., http://www.priv.gc.ca/information/research-recherche/2011/barrigar_201102_e.asp (last modified Mar. 28, 2013).

179. Telephone Interview with Ken Klingenstein, *supra* note 80.

180. *Id.*

181. For instance, the United Kingdom is developing an "Identity Assurance Program" that Smedinghoff

develop in unique ways due to significant cultural differences related to attitudes about information privacy,[182] they may ultimately be interoperable.

VII. CONCLUSION AND REMAINING CHALLENGES

The IDESG trust mark system and David's data system do not fully resolve the important policy issues associated with power disparities, information security, and valuable data flows, but they take an important step forward in addressing these issues and the privacy harms associated with them. Relatedly, they offer a much-improved and workable alternative to our status quo system of notice and consent by attempting to locate equilibrium within Solove's "elaborate dance between self-management and paternalism."[183]

These systems preserve our liberal preference for individual control because users may choose to rely on trust marks and contracts with IdPs, through which individuals may share their personal data if they desire to do so. However, these systems are intended to simplify individuals' privacy choices. They provide *mildly* paternalistic guidance through trust marks and IdPs with which individuals may co-manage their data decisions. As noted above, Solove's dance will be ongoing, but the IDESG trust mark and David's data system demonstrate one way to start resolving the important tension that Solove highlights.

Much work remains to be done, though. The IDESG must develop clear standards for its trust mark if it is to be more useful than the BBB's accreditation. Arguably, the structure of the NSTIC better situates it to develop such standards. In addition, the NSTIC must determine how to audit for compliance with such standards, how standards should evolve with technology, and how to ensure that IdPs do not abuse their control of personal information. Clear standards must also be developed for "de-identified data" in the FIM context. Federal regulations like HIPPA may serve as useful examples in developing such data de-identification standards.

considers promising. Telephone Interview with Tom Smedinghoff, *supra* note 47.

182. According to Klingenstein, projects are already developing in disparate ways. For instance, Europeans are much more comfortable with governments setting privacy standards than are Americans, who prefer the private sector to develop such standards. Telephone Interview with Ken Klingenstein, *supra* note 80.

183. Solove, *supra* note 18, at 19.