# FINDING THE BEST OF THE IMPERFECT ALTERNATIVES FOR PRIVACY, HEALTH IT, AND CYBERSECURITY

PETER SWIRE*

Neil Komesar's book *Imperfect Alternatives* is an excellent guide to those perplexed by information policy issues, namely health privacy, electronic health records (EHRs), Internet privacy, and cybersecurity. This Article begins by applauding Komesar's insistence, all too rare in political debates, that there are significant market failures and government failures. It then builds on Komesar's approach to assess the Health Insurance Portability and Accountability Act (HIPAA) medical privacy rule, the 2009 support for EHRs in the stimulus law, the current Internet privacy debates, and the ongoing debates about whether federal legislation is needed for cybersecurity.

First, the HIPAA privacy rule illustrates how one approach may be the best available, even with its known flaws. Despite plenty of warts as HIPAA went into effect, my judgment a dozen years later is that it was appropriate to create national health privacy standards by regulation.

Second, the apparent success of the 2009 health IT funding illustrates how government action can overcome market failures caused by the difficulty and cost of coordinating among numerous actors. The stimulus bill provided $19 billion as incentives for providers to shift to electronic clinical records. My judgment is that the financial incentives and meaningful use standards have kickstarted a major new round of adoption of EHRs.

Third, the Internet privacy discussion shows serious enough flaws in the market/self-regulatory approach to make legislation appear preferable. For the initial phase of the Internet, through the late 1990s, I believe the best choice quite possibly was the position taken by President Bill Clinton's administration. The policy was to encourage industry self-regulation, backed up by Federal Trade Commission enforcement if industry fell short of its promises. Today, however, there is now an infrastructure to write, enforce, and comply with baseline privacy rules for the Internet.

Fourth, the cybersecurity discussion reminds us that government failures may outweigh market failures even where some market failures are apparent. The pessimistic conclusion that legislation cannot cause any real

---

* C. William O'Neill Professor of Law at the Moritz College of Law of The Ohio State University and Senior Fellow, Future of Privacy Forum. This Article was prepared for the *Wisconsin Law Review* Symposium in honor of the work of Neil Komesar. Thanks to Yianni Lagos for research assistance. For research support, thanks to the Moritz College of Law and the Future of Privacy Forum, which receives financial support from a wide array of organizations, including software and online companies that are affected by the issues discussed in this Article. The views expressed here are those of the author, and were developed without specific funding or consultation with supporters of the Future of Privacy Forum.

> increase in security leaves me, at this time, without a convincing strategy for improving cybersecurity on the Internet.
>
> Finally, the discussion of adjudication shows that courts are unlikely to be the appropriate institution for many issues of privacy, security, or health information technology. Courts are relatively good at adjudicating whether a specific violation has occurred in the past; they are much less effective at guiding the design of complex technological systems that evolve rapidly.



## INTRODUCTION

In 2003, I taught one of the first law school courses on "The Law of Cybersecurity." The main text for the course was a book that does not even mention cybersecurity: Neil Komesar's *Imperfect Alternatives: Choosing Institutions in Law, Economics, and Public Policy*.[1] No textbook yet existed about the legal responses to malware, bots, denial of service attacks, and the other technical aspects of cybersecurity. Komesar's book, however, was the single best vehicle I could find to prepare my students to think critically about comparative institutional analysis, such as how to create institutions that foster better cybersecurity. I am thus delighted to have the opportunity to contribute to this Symposium honoring Komesar and his work.

This Article applies Komesar's approach to a range of information policy issues, namely health privacy, electronic health records (EHRs), Internet privacy, and cybersecurity. As a law professor since 1990, I have written extensively about these issues.[2] I have also had the good fortune

1. NEIL K. KOMESAR, IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS, AND PUBLIC POLICY (1994).

2. For a full list of publications, see *Peter Swire*, PETERSWIRE.NET, http://www.peterswire.net/pspublications.htm (last visited Feb. 24, 2013).

to experience these issues in practice, as a practicing lawyer[3] and in two roles in government: as Chief Counselor for Privacy under President Bill Clinton and as Special Assistant for Economic Policy under President Barack Obama. This Article thus seeks to blend theory and practice.

Komesar's work admirably balances pessimism and optimism. The pessimism comes from his acute awareness of the flaws in each institutional alternative, such as the market, a regulatory agency, or a court. The optimism comes from a conviction that thoughtful analysis can help us choose the best of these imperfect alternatives. Mark Twain wrote: "[t]he man who is a pessimist before forty-eight knows too much; if he is an optimist after it, he knows too little."[4] This quote captures my own feelings for how Komesar's analysis applies to Washington. Somehow we should strive to meld the optimism and the energy of the young with the wisdom and knowledge of imperfection of those no longer young.

This Article begins by applauding Komesar's insistence, all too rare in political debates, that we be aware of both market failures and government failures. It then builds on Komesar's approach to assess the Health Insurance Portability and Accountability Act (HIPAA) medical privacy rule, the 2009 support for EHRs in the stimulus law, the current Internet privacy debates, and the ongoing debates about whether federal legislation is needed for cybersecurity. This Article concludes by examining the role of the courts in these information policy issues. Courts have comparative expertise at adjudicating specific instances of alleged wrongdoing; they are far less effective, however, at designing the complex technological systems at the heart of these information policy debates.

## I. KOMESAR AS "RAGING MODERATE": MARKET FAILURES AND GOVERNMENT FAILURES

> *[T]he test of a first-rate intelligence is the ability to hold two opposed ideas in the mind at the same time, and still retain the ability to function.*
>
> —F. Scott Fitzgerald[5]

3. I practiced from 1986 to 1990 as a full-time associate in the Washington, D.C. office of Powell, Goldstein, Frazer & Murphy, and from 2001 to 2008 as a consultant to the Washington, D.C. office of Morrison & Foerster, LLP.

4. ALBERT BIGELOW PAINE, MARK TWAIN: A BIOGRAPHY, VOLUME II 744 (1912).

5. F. Scott Fitzgerald, *The Crack-Up*, *in* THE CRACK-UP 69, 69 (Edmund Wilson ed., New Directions 1945).

> *[S]ingle institutional analysis has largely served one-sided calls for political intervention (in the case of welfare economics) or against political intervention (in the case of public choice).*
>
> —Neil Komesar[6]

Washington policy debates often boil down to two sides, a battle between those who see market failures and those who see government failures. As Komesar writes, the market failure perspective comes from welfare economics, which often uses environmental pollution as a prime example. A factory gets all the profits from its production, but creates externalities by polluting the air. To solve the market failure, the answer is to pass the Clean Air Act. The market returns to efficiency because the factory now pays for the actual costs of its production. For privacy, a classic market failure is that the company overcollects personal information, but does not internalize the costs to the individual whose privacy is invaded or data is lost. For those trained in market failures, the task is to figure out how to write the modern-day equivalent of the Clean Air Act. The new law will provide the right incentives for privacy, improve overall efficiency, and avoid the unfair and negative effects caused by pollution or secret data collection.

On the other side, many in Washington are by now highly expert in pointing out government failures—the ways that even well-intentioned regulations go wrong. Public choice scholars write that many government regulations are examples of interest groups grabbing for rents through the political process, rather than the idealized correction of market failures that the welfare economists imagine. Prominent think tanks such as the American Enterprise Institute and the Heritage Foundation criticize a panoply of proposed regulations. On this view, environmental regulations kill jobs by imposing regulatory burdens far in excess of public health benefits. Privacy rules can destroy the financial underpinnings of the online economy by preventing well-targeted ads.

Both sides of this debate have their slogans. President Reagan famously summarized the government failure argument: "the nine most terrifying words in the English language are 'I'm from the government and I'm here to help.'"[7] More recently, President Obama pointedly joked about the knee-jerk answers of the antiregulatory crowd: "Feel a cold

---

6. KOMESAR, *supra* note 1, at 274.
7. Helen Thomas, *Washington Window*, BRYAN TIMES, Aug. 21, 1986, at 4.

coming on? Take two tax cuts, roll back some regulations, and call us in the morning."[8]

Furthermore, those involved in Washington policy debates have strong incentives to stick to their market-failure or government-failure lines. If you are trying to enact environmental or privacy protections in the face of opposition, then you are well served to have Rachel Carson write a passionate exposé about the perils of DDT or quote from one of many vividly titled books about how privacy is at risk.[9] Also, advocates who start to win are known to "move the goalposts"—they often (quite sincerely) believe that the status quo is not nearly protective enough, so it makes sense to push and ask for more whenever there is an opportunity. On the government-failure side, the incentives are similar. In any debate, why acknowledge any market failure when you can spend your time instead talking about how the proposal will kill jobs, suppress innovation, and place us on the slippery slope to the nanny state?

Neil Komesar's book offers reason and common sense to replace these one-sided analyses. Following in the tradition of Ronald Coase, he explains the many market failures and transaction costs that can occur in unregulated markets. At the same time, Komesar's institutional approach acknowledges the many ways that government efforts can reduce efficiency or otherwise go wrong. Compared to the one-sided briefs written in Washington policy battles, Komesar in my view gets it right: there are significant market failures *and* government failures.

That is why I compare Komesar to F. Scott Fitzgerald's description of a first-rate mind: "the test of a first-rate intelligence is the ability to hold two opposed ideas in the mind at the same time, and still retain the ability to function."[10] Komesar retains the ability to function by doing comparative institutional analysis. He recommends a patient, openminded, and realistic effort to understand how markets and regulations really work: "Institutional choice is difficult as well as essential. The choice is always a choice among highly imperfect alternatives."[11] The imperfections of markets and regulators often

---

8. Remarks Accepting the Presidential Nomination at the Democratic National Convention in Charlotte, North Carolina, 1 PUB. PAPERS 693 (Sept. 6, 2012).

9. *See, e.g.*, SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY (Deborah Russell & Madeleine Newell eds., 2000); ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS (1971); JON L. MILLS, PRIVACY: THE LOST RIGHT (2008); GINI GRAHAM SCOTT, THE DEATH OF PRIVACY: THE BATTLE FOR PERSONAL PRIVACY IN THE COURTS, THE MEDIA, AND SOCIETY (2011); CHARLES J. SYKES, THE END OF PRIVACY (David Stanford Burr ed., 1999); REG WHITAKER, THE END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY (1999).

10. FITZGERALD, *supra* note 5, at 69.

11. KOMESAR, *supra* note 1, at 5.

overlap: "[T]he same factors that change the ability of one institution across two situations very often change the ability of its alternative (or alternatives) in the same direction. Quite commonly, albeit not always, institutions move together."[12] Hence, the wisest course may be to choose a path that has known and significant flaws: "tasks that strain the abilities of an institution may wisely be assigned to it anyway if the alternatives are even worse."[13]

Rereading *Imperfect Alternatives* reminded me of Al Gore's famous (and famously lampooned) line about being a "raging moderate."[14] Komesar's writings show passion for solving the difficult problems of our day. He writes: "[m]y ultimate goal is to aid the reformation of society."[15] Not for Komesar, however, are the easy nostrums of either the left or the right. He knows that "[t]he vision of institutions in this book is not heartening."[16] Yet he holds out hope that the hard work of institutional analysis can improve society: "there are moments when selective and focused action can be telling."[17] And public service remains a potentially noble calling: "[p]ublic-interested public officials may not dominate these processes, but they can matter."[18]

In my own scholarship and other work, I confess to having precisely these "raging moderate" tendencies. Some of my writings strongly criticize privacy laws where they seem to me overly strict or insufficiently attentive to other values.[19] In other settings, I argue that legal protections for privacy are essential,[20] and that regulatory critics overstate the problems and costs of privacy protections.[21] I try to keep

---

12. *Id.* at 23.

13. *Id.* at 6.

14. DALE ANDERSON & AL GORE, A WAKE-UP CALL TO GLOBAL WARMING 21 (2009).

15. KOMESAR, *supra* note 1, at 274.

16. *Id.*

17. *Id.*

18. *Id.*

19. *See, e.g.*, PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 17 (1998); Peter P. Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, MD. L. REV. (forthcoming 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2159157.

20. *See, e.g.*, Peter P. Swire, *Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy*, 54 HASTINGS L.J. 847 (2003); FTC, SUMMARY OF PRESENTATION BY PETER SWIRE (2004), http://ftc.gov/os/meetings/040205swire.pdf.

21. Peter P. Swire, *New Study Substantially Overstates Costs of Internet Privacy Protections*, PETERSWIRE.NET (May 9, 2001), http://www.peterswire.net/hahn.html; Peter Swire, William O'Neill Professor of Law, Moritz College of Law, The Ohio State Univ., The Need for Privacy Protections: Is

the "opposed ideas" of market failure and government failure in mind at the same time, and do the comparative institutional analysis that Komesar advocates.

On an optimistic note, I also suggest that Komesar's approach is more thoroughly institutionalized in the U.S. government than most would suspect. Komesar summarizes his approach in this way: "I frequently discuss these institutional choices against a background of something roughly akin to resource allocation efficiency."[22] I submit that "something roughly akin to resource allocation efficiency" is an apt description of the approach to cost-benefit analysis employed by the United States Office of Management and Budget (OMB) for review of proposed regulations. President Obama issued Executive Order 13,563 in 2011, building on the cost-benefit approaches approved by all the Presidents since Jimmy Carter.[23] Work on this executive order was led by Cass Sunstein, in his role as Administrator of the Office of Information and Regulatory Affairs at the OMB. Sunstein described the Executive Order in the language of allocative efficiency: "we must promote predictability and reduce uncertainty, consider both costs and benefits, and use the least burdensome tools to achieve ends."[24] At the same time, the goal is only "roughly" about efficiency. Executive Order 13,563 expanded the list of intangible factors that OMB would consider: "[w]here appropriate and permitted by law, each agency may consider (and discuss qualitatively) values that are difficult or impossible to quantify, including equity, human dignity, fairness, and distributive impacts."[25] In re-reading Komesar's book while preparing this Article, the new list is a close match with the nonefficiency issues considered by Komesar in *Imperfect Alternatives*.

---

Industry Self-Regulation Adequate? (June 28, 2012) (transcript of statement before the Senate Committee on Commerce, Science, and Transportation), *available at* www.peterswire.net/senate%20commerce.swire.062712.docx.

22. KOMESAR, *supra* note 1, at 49–50.

23. Exec. Order No. 13,563, 76 Fed. Reg. 3821 (Jan. 18, 2011); CURTIS W. COPELAND, CONG. RESEARCH SERV., R41974, COST-BENEFIT AND OTHER ANALYSIS REQUIREMENTS IN THE RULEMAKING PROCESS 7 (2011), http://www.fas.org/sgp/crs/misc/R41974.pdf.

24. *Office of Information and Regulatory Affairs: Federal Regulations and Regulatory Reform under the Obama Administration: Hearing Before the Subcomm. on Courts, Commercial and Administrative Law of the H. Comm. on the Judiciary*, 112th Cong. 14 (2012) (statement of Cass R. Sunstein, Administrator, Office of Information and Regulatory Affairs).

25. *See* Exec. Order No. 13,563, *supra* note 23, at 3821. For an analysis of the changes from previous practice, see *Obama Review of Regulatory Burden to Be Weighed in Cost-Benefit Analysis*, SIDLEY AUSTIN LLP, 3 (Feb. 24, 2011), http://www.sidley.com/Obama-Review-of-Regulatory-Burden-to-Be-Weighed-in-Cost-Benefit-Analysis-02-24-2011 (from website, follow hyperlink to view document as PDF).

## II. IMPERFECT ALTERNATIVES FOR MEDICAL PRIVACY: THE HIPAA PRIVACY RULE

> *[T]asks that strain the abilities of an institution may wisely be assigned to it anyway if the alternatives are even worse.*
>
> —Neil Komesar[26]

I was the White House coordinator for the draft HIPAA privacy rule issued in September 1999 and the final regulation issued in December 2000. After leaving government, I consulted with a law firm, helping covered entities such as a research hospital and a medical device manufacturer create their HIPAA compliance programs. During the compliance phase, I got used to ducking away and protectively hunching my shoulders when people learned I was one of the guys who had created the HIPAA mess. A couple of times I literally had things thrown at me, but they were soft and thrown (mostly) in jest.

As HIPAA went into effect, some of the complaints struck me as the sort of griping people do when they know they have to do an unpleasant task but they understand that they have to do it. The first time typical people sit down to a regulatory training program on HIPAA, for instance, they can think of a very long list of things they would rather be doing. Deep down, however, they quite possibly realize that they should learn how to keep patient records confidential and secure. Medical data is widely understood to be especially sensitive, and the idea of medical confidentiality is even included in the Hippocratic Oath.[27]

With that said, the 2000 final HIPAA regulation had flaws and to this day creates some significant problems. For instance, that rule made it seem unlawful for friends and family members to pick up prescriptions at the pharmacy for a patient (that was fixed in the 2003 revised rule).[28] The 2000 rule had rules for accounting for patient records that were difficult to manage and gave little privacy benefits (those were fixed in 2003 as well).[29] The HIPAA notices have become a ritual when you see a new doctor but do not do much to actually inform patients about their choices. More difficult for lawyers to intuit, my engineering friends have emphasized how much difficulty was caused by having terms like

---

26. KOMESAR, *supra* note 1, at 6.

27. *Hippocratic Oath*, CORNELL.EDU, http://www.med.cornell.edu/deans/pdf/hippocratic_oath.pdf ("That whatsoever I shall see or hear of the lives of my patients that is not fitting to be spoken, I will keep in confidence.").

28. *Compare* Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. §§ 160, 164 (2001), *with* Health Insurance Reform: Security Standards, §§ 160, 162, 164 (2004).

29. *See* Health Insurance Reform: Security Standards, §§ 160, 162, 164 (2004).

"reasonable" included in the rule; it turns out that it is exceedingly hard to write compliance software for "reasonable and appropriate" protection of electronic health information.[30] The marketing rules were very difficult to understand. The research rules were well intended, and permit many kinds of medical research to go forward smoothly, but they likely do create important obstacles to medical research in some instances. Perhaps most strikingly for someone involved in writing the rule, it was interpreted initially by many lawyers and consultants to be far stricter than we authors had intended. Part of that was natural caution in the face of an uncertain new regulatory regime. As I watched compliance occur nationwide, part of it also seemed to be a strategic decision by lawyers and consultants to take the most conservative possible reading of the rule. That would make their compliance advice more important and increase the compliance fees.

In short, I saw plenty of warts as HIPAA went into effect. With that said, I remain convinced that the HIPAA privacy rule was an appropriate institutional choice. I have previously written a step-by-step history of how and why the HIPAA privacy rule was promulgated.[31] One key point is that the HIPAA privacy and security rules were part of the overall shift to electronic billing records in health care.[32] Once medical records were becoming electronic and easily shared nationwide, it made sense to have national privacy and security protections as well. The other key point is that Congress gave little guidance to the United States Department of Health and Human Services (HHS) about the content of the privacy rule. It was not for lack of effort, however. The 1996 law gave Congress until August 1999 to write a medical privacy law.[33] Congress in those days had a strong incentive to do so—the Republicans controlled the House and the Senate, and did not want to give wide discretion to the Democratic administration. Even with that incentive, however, no bill emerged from either a subcommittee or committee in either chamber.

---

30. *See* § 164.306(d)(3)(i) (2007). Other examples in the rule include: (1) "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a)," § 164.308(a)(1)(ii)(B); (2) "Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it," § 164.314(a)(2)(i)(B); (3) "[M]ake reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request," § 164.502(b)(1).

31. Peter Swire, *Medical Privacy*, PETERSWIRE.NET, http://www.peterswire.net/psmedicalpage.htm (last visited Feb. 22, 2013).

32. *Id.*

33. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264(c)(1), 110 Stat. 1936, 2033 (1996); *see also* Swire, *supra* note 31.

The issues were too difficult, Congress was not able to act, and HHS in 1999 came under a legal obligation to promulgate the rule.[34]

In conclusion on HIPAA, my judgment a dozen years later is that it was appropriate to create national health privacy standards by regulation. Most of the HIPAA provisions today seem like common sense—patients should have basic confidentiality protections when they receive medical care, and those protections should be built directly into the computer systems. I am proud that patients now have strong access rights to their medical records, which was often not true prior to the regulation. And the changes to HIPAA since 2000 have been modest corrections, rather than the large overhauls that would have been needed if the 2000 regulation had been drastically flawed. With apologies for any personal bias, I do not see any other institutional approach that would have done nearly so well.

## III. IMPERFECT ALTERNATIVES FOR PROMOTING ELECTRONIC HEALTH RECORDS: SOLVING COORDINATION PROBLEMS

> *[Comparative institutional] analysis converges with Ronald Coase's famous transaction cost approach.*
>
> —Neil Komesar[35]

> *[T]here are high costs of transacting in most settings.*
>
> —Neil Komesar[36]

The biggest challenge for Electronic Health Records (EHRs) is how to create standards that can be used by the numerous and diverse actors in the U.S. medical system. Presidents in recent years have agreed that the United States should rapidly develop the use of EHRs. For instance, President George W. Bush in 2004 announced the intention to provide an electronic health record to every U.S. resident by 2014.[37] President Barack Obama concurred: "[w]e will make the immediate investments necessary to ensure that within five years all of America's medical records are computerized."[38] EHRs can improve the quality of medical care, for example by automatically checking for allergies before a

34. § 264(c)(1), 110 Stat. at 2033; *see also* Swire, *supra* note 31.

35. KOMESAR, *supra* note 1, at 99.

36. *Id.* at 112.

37. Remarks in a Discussion at Vanderbilt University Medical Center in Nashville, Tennessee, 2004 PUB. PAPERS 933, 935 (May 27, 2004).

38. Commentary, *Bovard: Great Medical Records Round up*, WASH. TIMES (Mar. 13, 2009), http://www.washingtontimes.com/news/2009/mar/13/great-medical-records-roundup/?phpMyAdmin=Wne8EMI5OWl7AMIRBjANs94K-y4.

prescription is issued. A medical information network can also create benefits similar to the interstate highway system—creation of better infrastructure enables myriad uses that are difficult to predict in advance.[39]

Despite this bipartisan consensus and presidential-level attention, widespread use of EHRs has been slower than hoped. Based on my work with the Markle Foundation's Connecting for Health project,[40] my view is that high bargaining and other transaction costs have blocked adoption of private-sector standards. It was very difficult to solve coordination problems until the government: (1) provided significant financial incentives for providers to adopt EHRs and (2) promulgated standards rather than waiting for private-sector standards organizations to reach consensus. The 2009 stimulus bill, the American Recovery and Reinvestment Act, addressed both of these problems.[41]

HIPAA essentially spurred the use of electronic records for payment but not for clinical purposes. Along with the HIPAA privacy and security rules, the law mandated HHS to write what is called the "transaction and code set rule."[42] This rule responded to industry complaints that there was not enough standardization in the electronic formats used to submit payment requests for Medicare and other federal payments. In the absence of standardization, covered entities were reluctant to invest in costly information technology that was compatible with some but not other formats required to receive payment. In addition, the lack of standardization was a barrier to new entrants, reducing competition and raising costs. The cost-benefit analysis for the transaction and code set rule projected over $20 billion in net benefits over ten years.[43]

Implementation of the transaction and code set rule, unsurprisingly to a student of Komesar's writings, was imperfect. In my own work during that period, the complaint that I heard most often was that insurance companies and others achieved less standardization than the

---

39. For discussion of the positive externalities of building infrastructure, see BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES (2012).

40. I was one of many researchers and industry experts who worked with Connecting for Health during the Bush administration. *See generally Connecting for Health*, MARKLE, http://www.markle.org/health/connecting-health (last visited Feb. 23, 2012).

41. *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, §§ 13001–301, 123 Stat. 115, 226–58 (2009).

42. AM. MED. ASS'N, UNDERSTANDING THE HIPAA STANDARD TRANSACTIONS: THE HIPAA TRANSACTIONS AND CODE SET RULE (2009), *available at* http://www.ama-assn.org/resources/doc/psa/hipaa-tcs.pdf.

43. Health Insurance Reforms: Standards for Electronic Transactions, 65 Fed. Reg. 50,312, 50,345 (Aug. 17, 2000).

rule contemplated. The reason I heard was that this fended off competition for processing payments.[44] Despite these imperfections, the vast majority of federal health care reimbursements now take place in electronic form.[45]

The same cannot be said for clinical records. Under President Bush, shifting to EHRs was a stated priority of the administration and HHS.[46] In 2004, President Bush created the Office of the National Coordinator for Health Information Technology to spur development and adoption of EHR standards.[47] Much of the focus was on defining standards to make it easy for patient records to be shared within Regional Health Information Associations, as well as between regions in a proposed National Health Information Network.[48]

The basic strategy during the Bush administration was to use the government to focus attention on the need for EHRs, and encourage the private sector and standard organizations to take the lead. Despite ongoing speeches and other support for EHRs from President Bush and HHS Secretary Tommy Thompson, actual progress was disappointingly slow.[49] In 2001, approximately eighteen percent of office-based physicians used EHRs.[50] By 2008, that portion had increased only to forty-two percent.[51] One exception to this story of slow adoption was the Veterans Administration (VA), which won public praise for its early and

---

44. *See* UNDERSTANDING THE HIPAA STANDARD TRANSACTIONS, *supra* note 42, at 4–5 (discussing the implementation of the transaction and code set rule).

45. *See, e.g.*, *Electronic Billing Process*, MED. TRANSCRIPTION COMPANIES, http://www.topmedicaltranscription.com/Content25/Electronic-Billing-Process.htm (last visited Feb. 23, 2013).

46. *See* Remarks in a Discussion at Vanderbilt University Medical Center, *supra* note 36, at 933–36.

47. Jaan Sidorov, *It Ain't Necessarily So: The Electronic Health Record and the Unlikely Prospect of Reducing Health Care Costs*, 25 HEALTH AFF. 1079, 1079 (2006).

48. *See, e.g.*, *Regional Health Information Organizations*, AM. OPTOMETRIC ASS'N, http://www.aoa.org/x6529.xml (last visited Feb. 23, 2013).

49. *See* Sidorov, *supra* note 47; Jonathan M. Gitlin, *Study: US Adoption of Electronic Health Records Is Abysmal*, ARS TECHNICA (June 19, 2008), http://arstechnica.com/uncategorized/2008/06/study-us-adoption-of-electronic-health-records-is-abysmal/; News Release, U.S. Dep't of Health & Human Servs., HHS Launches New Efforts to Promote Paperless Health Care System (July 1, 2003), http://www.nih.gov/news/pr/jul2003/nlm-01.htm.

50. CHUN-JU HSIAO ET AL., CTRS. FOR DISEASE CONTROL AND PREVENTION, NCHS DATA BRIEF: ELECTRONIC HEALTH RECORD SYSTEMS AND INTENT TO APPLY FOR MEANINGFUL USE INCENTIVES AMONG OFFICE-BASED PHYSICIAN PRACTICES: UNITED STATES, 2001-2011, at 1 fig.1 (2011), *available at* http://www.cdc.gov/nchs/data/databriefs/db79.htm.

51. *Id.*

effective use of EHRs.[52] The VA system was unusual in health care because of its scale and centralized administration; the relative success of the VA suggested that coordination among institutions was a key barrier to use of EHRs.

The Obama administration adopted a different strategy. The stimulus bill provided $19 billion as incentives for providers to shift to electronic clinical records.[53] To qualify for the payments, covered entities had to achieve "meaningful use" of EHRs.[54] HHS has since promulgated two rounds of regulations defining "meaningful use."[55]

My judgment is that the financial incentives and meaningful use standards have kickstarted a major new round of adoption of EHRs. I base this judgment in part on anecdotes—my own family physician finally shifted to EHRs in early 2012 and experts in the field tell me that higher adoption is finally occurring. The statistics, although early to be determinative, show the same trend.

> Among physician practices, the percentage with at least a basic electronic health record system grew steadily from the 17 percent in late 2007/early 2008 to 35 percent in 2011.
>
> . . . .
>
> The percentage of hospitals with at least a basic electronic health record system increased slowly from late 2007/early 2008 (9.1 percent) through 2010 (15.1 percent).[56]

The financial incentives provide a visible and credible promise that a provider will benefit from shifting to EHRs. In addition, the meaningful use standards create a credible promise that EHRs will be interoperable. Providers who meet the standards are not likely to be stranded with a noncompliant system.

---

52. *See, e.g.*, Chelsey Ledue, *VA a Good Model for EHR Systems and Implementation*, HEALTHCARE IT NEWS (Apr. 6, 2009), http://www.healthcareitnews.com/news/va-good-model-ehr-systems-and-implementation.

53. Emily P. Walker, *Senate Passes Stimulus Bill with $19 Billion for Health IT*, MEDPAGE TODAY (Feb. 11, 2009), http://www.medpagetoday.com/Washington-Watch/Washington-Watch/12843.

54. Andy Kessler, *A Pound of Cure*, MIT TECH. REV. (June 23, 2009), http://technologyreview.com/review/414031/a-pound-of-cure/.

55. *Meaningful Use*, HEALTHIT.GOV, http://www.healthit.gov/policy-researchers-implementers/meaningful-use (last visited Feb. 23, 2013).

56. ROBERT WOOD JOHNSON FOUNDATION, MEASURING ADOPTION AND USE OF HEALTH INFORMATION TECHNOLOGY TO REDUCE HEALTH CARE DISPARITIES AND IMPROVE QUALITY: A PROGRESS REPORT: 2006-2013, at 7 (2012) (citations omitted), *available at* www.rwjf.org/content/rwjf/en/research-publications/find-rwjf-research/2012/08/measuring-adoption-and-use-of-health-information-technology-to-r.html.

## IV. IMPERFECT ALTERNATIVES FOR INTERNET PRIVACY: WHY SELF-REGULATION IS NO LONGER ENOUGH

> *Good heavens! For more than forty years I have been speaking prose without knowing it*.
>
> —Molière[57]

Internet privacy is a challenging issue for comparative institutional analysis. In 1997, before I encountered Komesar's work, I wrote a paper for the United States Department of Commerce titled *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*.[58] The paper discussed both market and government failures at length, in ways that are consistent with Komesar's approach.[59] When I left government, and read *Imperfect Alternatives*, I had the realization that I had been speaking "prose" without knowing it, or, as Komesar called it, "comparative institutional analysis." Komesar had systematized and clearly explained ideas that I had been groping for in writing and in practice.

Privacy on the Internet faces both market and government failures. The 1997 article included this discussion about market failure:

> A chief failure of the market approach is that customers find it costly or impossible to monitor how companies use personal information. When consumers cannot monitor effectively, companies have an incentive to over-use personal information: the companies get the full benefit of the use (in terms of their own marketing or the fee they receive from third parties), but do not suffer for the costs of disclosure (the privacy loss to consumers).[60]

---

57. MOLIERE, LE BOURGEOIS GENTILHOMME, act 2, sc. 4 (as commonly translated).

58. Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (Nat'l Telecomms. & Info. Admin. 1997), http://www.ntia.doc.gov/report/1997/privacy-and-self-regulation-in-information-age. I am fairly certain that I had not read Neil Komesar's work by 1997. Our approaches were already quite similar at that time. By my 2003 course on The Law of Cybersecurity, I had discovered his work and relied on it to explain comparative institutional analysis to my students.

59. *Id.*

60. *Id.*

The article also explained that government failures are likely to be substantial—technology changes rapidly, the diversity of data uses is large, and the political process responds to well-funded lobbyists.[61]

For the initial phase of the Internet, through the late 1990s, I believe the best choice quite possibly was the position taken by the Clinton administration. The policy was to encourage industry self-regulation, backed up by Federal Trade Commission (FTC) enforcement if industry fell short of its promises. The 1997 paper emphasized that self-regulation works best when there is a credible threat that government will step in if industry does not do a good job.[62] During the late 1990s, the Clinton administration and the FTC discussed the possible need for legislation, and spurred industry to post privacy policies on their websites. Progress was quite rapid, with only fourteen percent of commercial websites having a privacy policy in 1998, but eighty-eight percent having them only two years later.[63]

After the attacks of September 11, 2001, political interest in privacy declined as emphasis shifted to security, antiterrorism, and information sharing. As I documented in 2012 Senate testimony, when the credible threat of government action eroded, new self-regulatory activity essentially ceased and many self-regulatory programs eroded as well.[64]

Privacy has returned to public attention, similar to the late 1990s when the issue often appeared on newspaper front pages. We are now in a second wave of global privacy protection.[65] We have experienced explosive growth in international data flows, online behavioral advertising, social networks, and mobile computing. The European Union has proposed a major overhaul of its 1995 privacy directive,[66] and comprehensive privacy laws have spread to numerous countries around the world.[67] In the United States, the Obama administration has proposed

---

61. *Id.*

62. *See id.*

63. Swire, *supra* note 20, at 863–65.

64. *The Need for Privacy Protections*, *supra* note 21, at 4.

65. Peter Swire, *Moving Too Fast on Cybersecurity*, HILL (Apr. 20, 2012, 10:36 AM), http://thehill.com/business-a-lobbying/222783-moving-too-fast-on-cybersecurity. The *Ohio State Law Journal* annual symposium for 2012 was titled "The Second Wave of Global Privacy Protection." *See Symposium*, OHIO ST. L.J., http://moritzlaw.osu.edu/students/groups/oslj/symposium-2/2012-2013-symposium (last visited Feb. 17, 2013).

66. *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, at 1–2, COM (2012) 11 final (Jan. 1, 2012).

67. *See* PETER P. SWIRE & KENESA AHMAD, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PROTECTION: A SURVEY OF GLOBAL CONCEPTS, LAWS AND PRACTICES (Terry McQuay ed., 2012).

a privacy bill of rights for online commerce,[68] and the FTC has pushed numerous privacy initiatives.[69]

Having lived through the ups and downs of Internet privacy debates for the past fifteen years, I believe that U.S. legislation is a sensible complement to industry self-regulation. We have seen the limitations of free-market and self-regulatory efforts, notably how industry effort diminished greatly once the spotlight turned to other issues. Compliance with privacy rules is far more mature than in the late 1990s. Sectors such as health care and financial services have had more than a decade of experience with what works and what does not under HIPAA and the Gramm-Leach-Bliley Act. The International Association of Privacy Professionals has grown from a tiny base to over 10,000 members.[70] In short, there is now an infrastructure to write, enforce, and comply with baseline privacy rules for the Internet.

## V. IMPERFECT ALTERNATIVES FOR CYBERSECURITY: FIRST, DO NO HARM

> *[T]he same factors that change the ability of one institution across two situations very often change the ability of its alternative (or alternatives) in the same direction. Quite commonly, albeit not always, institutions move together.*
>
> —Neil Komesar[71]

As my students learned in the 2003 class on The Law of Cybersecurity, there are major market failures as well as government failures for security against attacks made through the Internet. On the market failure side, cybersecurity often features an externality—the lack of good security by one organization creates losses for other parties. For instance, a user's computer might become a "bot"—a computer under the

68. Press Release, The White House Office of the Press Sec'y, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online (Feb. 23, 2012), http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

69. *See, e.g.*, FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.; PETER P. SWIRE & KENESA AHMAD, U.S. PRIVATE-SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS 15–16 (2012).

70. *About IAPP: Media*, INT'L ASS'N PRIVACY PROFESSIONALS (Mar. 7, 2012), http://privacyassociation.org/about_iapp/media/international_association_of_privacy_professionals_reaches_10000_member_mar.

71. KOMESAR, *supra* note 1, at 23.

control of a hacker. These bots are used to launch a high volume of attacks across the Internet, with negative effects far in excess of the harm to the computer that has become a bot. The networked and global nature of the Internet means that hackers can probe a huge number of systems in order to find the ones with weak security.

As Komesar teaches, the features that make an issue difficult for one institution (such as a market approach to cybersecurity) often make the issue similarly difficult for another institution (such as government rules for cybersecurity). One might hope, for instance, that the measures that seem to be working for EHRs might work in the cybersecurity instance. After all, both involve highly networked environments, and I suggested above that government could play a helpful role in overcoming obstacles to coordination for EHRs. My optimism is lower, however, for government cybersecurity rules. EHRs fundamentally create positive externalities—the more that the system uses high-tech EHRs, the greater the network effects and societal benefits. Once the EHR system is in place, cooperation will likely continue because the different systems can successfully communicate with each other. Cybersecurity, by contrast, features negative externalities: Alice's security flaw lets the hacker mount successful attacks on Bob's and others' systems. In this instance, system owners face continuing incentives to invest less in security than is societally optimal. In addition, many of the attacks originate outside of the United States, so law enforcement strategies often do not work.

One goal of government policy should be the online version of the Hippocratic Oath—first, do no harm.[72] Permitting widespread use of encryption is a prominent example for cybersecurity, because it is such an effective tool in many instances for blocking attacker access to communications and stored records.[73] In the 1990s, the United States placed limits on the export of effective encryption in order to make it easier for law enforcement and national security agencies to get access to communications.[74] The United States largely repealed those restrictions in 1999.[75] More recently, however, both China and India have considered or implemented limits on effective encryption.[76] As I have discussed

72. Susan Landau has emphasized the security vulnerabilities created on behalf of surveillance agencies, such as "back doors" to enable wiretaps. SUSAN LANDAU, SURVEILLANCE OR SECURITY? THE RISKS POSED BY NEW WIRETAPPING TECHNOLOGIES (2011).

73. Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 456 (2012).

74. *Id.* at 433–35.

75. *Id.* at 439–41.

76. *Id.* at 418.

elsewhere, the overall security of the Internet will be reduced if such encryption-blocking measures become widespread.[77]

It is trickier to say what laws or regulations would improve cybersecurity. The U.S. government does not play the dominant role in the Internet and cybersecurity that it does in U.S. health care, where the HIPAA security rule is basically similar in its effects to the privacy rule. Over ninety percent of the Internet's critical infrastructure is owned and operated by the private sector,[78] so there is limited leverage to have rules that apply to the government apply as well to the private sector. The U.S. government also supplies a negligible portion of funding related to online security, in contrast to its roughly forty-five percent share of U.S. health care dollars.[79] Without these tools that the government has in health care, the task of government regulation is quite difficult.

In my view, cybersecurity features acute market and government failures. In such instances, reasonable and informed people can differ on how to proceed. In contrast to my selection of a more prominent role for government in the previous discussions, I remain cautious about government regulation for cybersecurity.[80] My intuitions in this direction were strengthened by a recent one-on-one discussion with the Chief Information Security Officer (CISO) for one of the major U.S. banks. The CISO said that the greatest security value comes from the alerts shared through the industry's Financial Services Information Sharing and Analysis Center (FS-ISAC). The FS-ISAC coordinates rapid information sharing, especially among the largest and most-attacked financial institutions. Because attacks are so frequent and mutate so quickly, the defenses must adapt practically instantaneously. In discussing proposed cybersecurity legislation, the CISO said that he could see an increase in red tape, but no real increase in security, from the proposals.

This pessimistic conclusion leaves me, at this time, without a convincing strategy for improving cybersecurity on the Internet. First, we should do no harm. Also, we should encourage the close-knit groups of experts along the lines of the FS-ISAC. Beyond that, I welcome new and more optimistic insights.

---

77. *See id.* at 458–59.

78. NATIONAL INFRASTRUCTURE ADVISORY COUNCIL, CRITICAL INFRASCTRUCTURE PARTNERSHIP STRATEGIC ASSESSMENT 16 (2008).

79. Craig Eyermann, *Quick Facts on Federal Health Care Spending*, MYGOVCOST.ORG (Aug. 24, 2012, 7:47 AM), http://www.mygovcost.org/2012/08/24/quick-facts-for-federal-health-care-spending/.

80. Swire, *supra* note 65 (expressing skepticism of proposed cybersecurity bills).

## VI. THE LIMITED ROLE FOR THE COURTS IN GOVERNING INFORMATION SYSTEMS

> *In the adjudicative process, however, damages actions are largely retrospective*.
>
> —Neil Komesar[81]

The discussion thus far has focused on the strengths and failures in markets and regulatory agencies. Courts are the third alternative examined by Komesar. Adjudication is certainly an important feature in some settings. Courts are not a prominent alternative, however, for many issues of privacy, security, or health information technology. The basic reason is that these problems are not principally about individual redress for specific harms. Instead, the problems concern the design of technologically complex systems. Courts tend to do better at individual redress than at system design.[82] Among other reasons, courts are institutionally more expert at judging the facts of an incident than they are at intervening as managers over an extended period of time.

Consider some information policy issues that concern redress for specific harms. First, defamation is an example of a specific act that may cause damages. As Susan Freiwald has argued, comparative institutional analysis quite possibly supports an important role for courts in defining what constitutes defamation online.[83] The other traditional privacy torts similarly tend to involve a specific instance of alleged wrongdoing, such as intrusion on seclusion or public revelation of private facts. Second, the FTC has created a substantial body of consent decrees about what constitutes an "unfair or deceptive trade practice."[84] In most of these

---

81. KOMESAR, *supra* note 1, at 135.

82. I will not discuss this topic at length in this Article. The topic was a principal area of study early in my career, such as in my undergraduate thesis. *See* Peter M. Swire, The Onslaught of Complexity: Information Technologies and Developments in Legal and Economic Thought (Apr. 15, 1980) (unpublished B.A. thesis, Princeton University), *available at* http://www.peterswire.net/pspublications-unpub.htm. That thesis, in part, analyzed how well courts could intervene in complex ecological systems, such as pollution in Lake Superior. Owen Fiss was a leading proponent for the "structural reform" suit, where judges would play major roles in managing the education, prison, or other complex systems. Owen M. Fiss, *Foreword: The Forms of Justice*, 93 HARV. L. REV. 1, 44 (1979). Over time, however, this sort of broad judicial role to reform complex systems has become much less prominent than Fiss advocated.

83. Susan Freiwald, *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation*, 14 HARV. J.L. & TECH. 569, 573 (2001).

84. *See, e.g.*, Anne V. Maher & Lesley Fair, *The FTC's Regulation of Advertising*, 65 FOOD & DRUG L.J. 589, 592 (2010) (explaining the process the FTC uses in defining unfair and deceptive trade practices through consent decrees). *In the Matter of*

cases, the defendant allegedly made a specific promise and then broke it. Adjudication (and consent decrees settled in the shadow of adjudication) is well-suited to judge whether a promise has been broken. Third, part of the genius of the data breach laws is that the trigger for notification (and possible enforcement) is based on an adjudication-friendly question: was there a breach of the covered data in a way that triggers the law's notice requirements? Fourth, the neighboring realm of intellectual property is often different in this respect than the information policy issues addressed in this Article. Many intellectual property cases concern disputes that are analogous to property or other common-law issues. Did this license permit the behavior (interpretation of a contract)? Did this action infringe the owner's right (definition of a trespass)? Individual intellectual property cases often have implications for overall system design, but the shape of the case "feels" like traditional adjudication of the rights of the two parties.

Consider if courts tried to determine whether an Internet service offered "reasonable" privacy or cybersecurity. One challenge would be that systems and practices evolve very quickly on the Internet, so courts would often be looking at the antivirus and online advertising practices of a year or three before. Another challenge is the sheer complexity of data practices. Cybersecurity is based on "defense in depth," so that the system can continue to operate even if a few defenses are overcome. One bug in software or one password left exposed thus is not enough to show lack of reasonable care. In addition, one has to wonder about the technical competence of a lay jury or judge to assess the reasonableness of an organization's care.

The European Union's approach to privacy and data protection offers one alternative. Each member state has an independent data protection authority (DPA), one of whose tasks is to serve as an ombudsman and sometime enforcer of data practices.[85] Notably, a DPA can opine about whether a particular data practice meets the vague tests for the "legitimacy" and "proportionality" of data processing.[86] On the optimistic side, the DPA might gain technical expertise over time, and this role for the DPA can offer guidance to organizations about what is permissible. On the pessimistic side, the DPA gains considerable

---

*Facebook, Inc.*, File No. 0923184, Agreement Containing Consent Order, *available at* http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf.

85. *See* David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1, 12–13 (1999).

86. Olena Dmytrenko & Cara D. Cutler, *Does Ukraine Need a Comprehensive Statute to "Control" Private Data Controllers?*, 5 WASH. U. GLOB. STUD. L. REV. 31, 55–56 (2006).

discretion about what data practices are appropriate for online activities. However well the DPA approach works in Europe, my belief is that the U.S. political system is not ready to accept that level of independent agency discretion to pick winners and losers among online business activities.

## CONCLUSION

Komesar's book *Imperfect Alternatives* is an excellent guide to those perplexed by the issues of privacy, health IT, and cybersecurity. The information policy issues discussed here are plagued by significant market failures as well as government failures. Information policy issues are vitally important in our information age, but I suggest our passion should make us "raging moderates," caring deeply about the best answers but aware that each approach has flaws.

With those imperfections in mind, the issues analyzed here illustrate the importance and usefulness of Komesar's comparative institutional analysis. First, the HIPAA privacy rule illustrates how one approach may be the best available, even with its known flaws. Second, the apparent success of the 2009 health IT funding illustrates how government action can overcome market failures caused by the difficulty and cost of coordinating among numerous actors. Third, the Internet privacy discussion shows serious enough flaws in the market/self-regulatory approach to make legislation appear preferable. Fourth, the cybersecurity discussion reminds us that government failures may outweigh market failures even where some market failures are apparent. Finally, the discussion of adjudication shows that courts are unlikely to be the appropriate institution for many of these problems. Courts are relatively good at adjudicating whether a specific violation has occurred in the past; they are much less effective at guiding the design of complex technological systems that evolve rapidly.

Komesar closed his book by noting that "many are motivated to improve society" and "that serious and creative analyses of individual issues of law and public policy will add to and fill in the theory."[87] With the lessons from information policy in mind, perhaps a next round of scholars and actors will continue the work.

87. KOMESAR, *supra* note 1, at 275, 276.