Information Privacy:

Controversy Proposal Paper for the 2012-2013

Cross Examination Debate Association Topic Selection

By

Anonymous

Sample Resolutions:

Resolved: the United States federal government should substantially increase domestic protection(s) of the information privacy of real persons.

Resolved: the United States federal government should substantially increase domestic protection(s) of the information privacy and/or data privacy of real persons**.**

Defining the key terms "Information Privacy" and "real persons"

Professor Jerry Kang provides a working definition of the term "information privacy" that tends to fit the unique needs of the policy debate community. His definition is grounded in real policy task-forces' work products, and is used by academics, policy-makers, and the business community:

> Information privacy is "an individual's claim to control the terms under which personal information--information identifiable to the individual--is acquired, disclosed, and used." This definition comes from Principles for Providing and Using Personal Information ("IITF Principles"), issued by the Clinton administration's Information Infrastructure Task Force. I adopt the IITF's definition because it is analytically useful, consistent with a broad swatch of academic and policy thinking, and likely to be influential in governmental, private sector, and academic discussion. If history repeats itself, it will be the foundation for future federal privacy legislation (footnotes removed).[1]

The term "real persons" is a legal reference to distinguish real human beings from corporations. It functions to limit the intent of the resolution to protect the privacy rights of people, rather than shift the focus to corporations.

Harms and Inherency

Warren and Brandeis established the rationale for the American version of the Right to Privacy, the "right to be left alone," in the late 1800's.[2] Warren and Brandeis were particularly concerned with informational privacy. They were concerned that the new technologies of "instantaneous photographs and [the] newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'."[3] The technologies of the 21st Century again raise questions about the individual's right to be left alone. Professor Solove succinctly explains the nature of the multiple threats to individual informational privacy in 2002:

> Imagine that the government had the power to compel individuals to reveal a vast amount of personal information about themselves--where they live, their phone numbers, their physical description, their photograph, their age, their medical problems, all of their legal transgressions throughout their lifetimes whether serious crimes or minor infractions, the

> names of their parents, children, and spouses, their political party affiliations, where they work and what they do, the property that they own and its value, and sometimes even their psychotherapists' notes, doctors' records, and financial information.
>
> Then imagine that the government routinely poured this information into the public domain--by posting it on the Internet where it could be accessed from all over the world, by giving it away to any individual or company that asked for it, or even by providing entire databases of personal information upon request. In an increasingly "wired" society, with technology such as sophisticated computers to store, transfer, search, and sort through all this information, imagine the way that the information could be combined or used to obtain even more personal information.
>
> Imagine the ease with which this information could fall into the hands of crafty criminals, identity thieves, stalkers, and others who could use the information to threaten or intimidate individuals. Imagine also that this information would be available to those who make important decisions about an individual's life and career--such as whether the individual will get a loan or a job. Also imagine that in many cases, the individual might not be able to explain any concerns raised by this information or even know that such information was used in making these decisions.
>
> Imagine as well that this information would be traded among hundreds of private-sector companies that would combine it with a host of other information such as one's hobbies, purchases, magazines, organizations, credit history, and so on. This expanded profile would then be sold back to the government in order to investigate and monitor individuals more efficiently.
>
> Stop imagining. What I described is what is currently beginning to occur throughout the United States by the use of federal, state, and local public records, and the threat posed to privacy by public records is rapidly becoming worse.[4]

Solove explains the impact of these intrusions, "Consolidating various bits of information, each itself relatively unrevealing, can, in the aggregate, begin to paint a portrait of a person's life ... a 'digital biography.' A growing number of private sector organizations are using public records to construct digital biographies on millions of individuals ....These uses are resulting in a growing dehumanization, powerlessness, and vulnerability for individuals."[5] Joseph Kapkovic, citing Professor Solove and Amitai Etzioni, concludes:

> ["T]he privacy protections in the United States are riddled with gaps and weak spots .... In particular, emerging companies known as 'commercial data brokers' have frequently slipped through the cracks of U.S. privacy law." "An entire industry" has emerged that deals in the collection, processing, and dissemination of individuals' personal information, and it "is not well-regulated." This section will highlight several database applications effectuated by commercial data brokers.
>
> In his book *The Limits of Privacy*, Amitai Etzioni posits that most privacy threats that fail to serve the common good arise "not from the state, the villain that champions of privacy traditionally fear the most, but rather from the quest for profit by some private companies." Etzioni casts government intrusions upon privacy as necessary when balanced against a significant "common good" (e.g., drug testing those responsible for the lives of others--such

as public transportation drivers). He defines the "common good" as public safety and public health. "[W]hen courts and common parlance cite 'the public interest,' very often the reference is to matters that fall into one of these two pivotal categories."
According to Etzioni, "corporations now regularly amass detailed accounts about many aspects of the personal lives of millions of individuals, profiles of the kind that until just a few years ago could be compiled only by the likes of ... major state agencies, with huge staffs and budgets." Etzioni concludes his thoughts on what he has termed the privacy paradox by noting,
Although our civic culture, public policies, and legal doctrines are attentive to privacy when it is violated by the state, when privacy is threatened by the private sector our culture, policies, and doctrines provide a surprisingly weak defense. Consumers, employees, even patients and children have little protection from marketers, insurance companies, bankers, and corporate surveillance (footnotes removed).[6]

As one privacy rights group explains, "The United States has no federal privacy act to govern the collection, use and storage of personal information by the private sector. The Federal Trade Commission (FTC) is the only agency with authority over such information-gathering; and it can only enforce existing laws—it cannot create new ones….. In the United States, there have been attempts to draft legislation outlining fair information practices for online businesses; but nothing has yet passed into law. Instead, the industry regulates itself: companies draft their own privacy policies to explain how and why they collect personal information. As it stands right now, however, companies are not legally required to draft such policies."[7],[8] The Congressional Research Service has also concluded that there is no comprehensive federal protection for information privacy.[9]

Additionally, Associate Dean and Professor of Law, Hirsch, explains both the harms and the inherency regarding information privacy in the internet world:

First, new technologies are digitally collecting and tracking our social security numbers, reading habits, political beliefs, health issues, criminal histories, and other pieces of personal information as never before. Private businesses are then compiling and analyzing this data to put together comprehensive and invasive pictures of specific individuals. They use these "digital dossiers" to track our behavior and to market goods and services to us. Our ***6** "most intimate information [is being] circulated by an indifferent and faceless infrastructure." More nefariously, this "faceless infrastructure" employs the data to deny us jobs, credit, insurance, and other social goods, often without our knowledge. Making matters worse, the very fact that so much information is being collected and stored increases the chance that it will fall into the hands of those who would steal our identities to open credit cards, take out mortgages, or do worse in our names. These technological developments inhibit our ability to control our personal information and so injure our "informational privacy."
Second, the new damage to privacy does not end there. We also have a privacy interest in our personal spaces. This right to "spatial" privacy has traditionally protected us from intrusive behavior such as invasions of our homes or telephone calls that "are repeated with such persistence and frequency as to amount to a course of hounding the plaintiff." Today, the email inbox has become a place of social interaction as important as our living room or

phone line. The endless barrage of spam email "hounds" us in this personal space and damages our spatial privacy.
Just as the law had to adapt to changes during the Industrial Revolution, the law today is struggling to address the privacy damage of the Information Age. Many policymakers and legal scholars agree that the existing legal structure is insufficient to deal with the emerging injuries to privacy and that we need new laws capable of protecting personal privacy in the digital age (footnotes removed).[10]

Solvency Advocates.

Yes Virginia, it is possible to draft a viable policy debate topic that actually has real inherency, real harms and real solvency advocates--all at the same time. First and foremost, the Obama Administration proposed the "Consumer Privacy Bill of Rights" in February, 2012.[11] When it comes to "middle of the road" policy actions and solvency advocates, the Obama plan is as straight-forward as it gets:

> To address these issues, the Administration offers *Consumer Data Privacy in a Networked World*. At the center of this framework is a Consumer Privacy Bill of Rights, which embraces privacy principles recognized throughout the world and adapts them to the dynamic environment of the commercial Internet. The Administration has called for Congress to pass legislation that applies the Consumer Privacy Bill of Rights to commercial sectors that are not subject to existing Federal data privacy laws. The Federal Government will play a role in convening discussions among stakeholders—companies, privacy and consumer advocates, international partners, State Attorneys General, Federal criminal and civil law enforcement representatives, and academics—who will then develop codes of conduct that implement the Consumer Privacy Bill of Rights. Such practices, when publicly and affirmatively adopted by companies subject to Federal Trade Commission jurisdiction, will be legally enforceable by the FTC. The United States will engage with our international partners to create greater interoperability among our respective privacy frameworks. This will provide more consistent protections for consumers and lower compliance burdens for companies. Of course, this framework is just a beginning. Starting now, the Administration will work with and encourage stakeholders, including the private sector, to implement the Consumer Privacy Bill of Rights. The Administration will also work with Congress to write these flexible, general principles into law. The Administration is ready to do its part as a convener to achieve privacy protections that preserve consumer trust and promote innovation.[12]

Affirmative teams could adopt the White House's plan in total, or they could choose among the subset proposals. Here are sections of the various proposals:

> Codify the Consumer Privacy Bill of Rights
>
> Congress should act to protect consumers from violations of the rights defined in the Administration's proposed Consumer Privacy Bill of Rights. These rights provide clear protection for consumers and define rules of the road for the rapidly growing marketplace for personal data.42 The legislation should permit the FTC and State Attorneys General to enforce these rights directly. The legislation will need to state companies' obligations

under the Consumer Privacy Bill of Rights with greater specificity than this document provides. The Consumer Privacy Bill of Rights is a guide for the Administration to work collaboratively with Congress on statutory language. To provide greater legal certainty and to encourage the development and adoption of industry-specific codes of conduct, the Administration also supports legislation that authorizes the FTC to review codes of conduct and grant companies that commit to adhere—and do adhere—to such codes forbearance from enforcement of provisions of the legislation.[13]

…

Grant the FTC Direct Enforcement Authority

The Administration encourages Congress to grant the FTC the authority to enforce each element of the statutory Consumer Privacy Bill of Rights.44 This authority would provide greater certainty to consumers and companies both. Companies would begin with a clearer roadmap to their privacy obligations. Consumers would benefit from knowing that Congress has empowered the FTC to enforce a comprehensive set of privacy protections in the commercial marketplace. At the same time, a statute that allows the FTC to enforce the Consumer Privacy Bill of Rights directly would provide flexibility and permit the FTC to address emerging privacy issues through specific enforcement actions governed by applicable procedural safeguards. Companies seeking even greater certainty under such legislation should use the multistakeholder process and enforcement safe harbor discussed below to develop context-specific codes of conduct in a timely fashion. The Administration recommends that Congress grant the same authority to State Attorneys General. So long as they coordinate with the FTC in their enforcement actions, States could provide additional enforcement resources and a considerable source of consumer data privacy expertise.[14]

…

Provide Legal Certainty Through an Enforcement Safe Harbor

The Administration supports authorizing the FTC to provide greater assurance to companies that adopt enforceable codes of conduct than is possible under current law. Two legislative structures would help to accomplish this goal. First, the FTC should have explicit authority to review codes of conduct against the Consumer Privacy Bill of Rights, as they are set forth in legislation. Legislation should require the FTC to review codes submitted for review within a reasonable amount of time (e.g., 180 days), require the FTC to consider public comments on a code, limit its review authority to approving or rejecting a code that reflects the consensus of all participants in the multistakeholder process, and establish a period for reviewing approved codes to ensure that they sufficiently protect consumer privacy in light of technological and market changes. The record from the multistakeholder process that produced a code—and particularly the presence of general consensus on its provisions—would help to guide the FTC's assessment of whether a code sufficiently implements the Consumer Privacy Bill of Rights. Because the outcome of FTC review will likely influence companies' decisions to

adopt codes of conduct—the end result of the multistakeholder process—it is appropriate to determine the details of FTC review through a process that is open to all stakeholders. These details, however, need to be legally binding. Accordingly, the Administration recommends that Congress grant the FTC authority under the Administrative Procedure Act (5 U.S.C. § 552 *et seq.*) to issue rules that establish a fair and transparent process for reviewing and approving codes of conduct. The second element that the Administration recommends is giving the FTC the authority to grant a "safe harbor"—that is, forbearance from enforcement of the statutory Consumer Privacy Bill of Rights—to companies that follow a code of conduct that the FTC has reviewed and approved. Companies that decline to adopt a code of conduct, or choose not to seek FTC review of a code that they do adopt, would simply be subject to the general obligations of the legislatively adopted Consumer Privacy Bill of Rights.[15]

…

D. Balance Federal and State Roles in Consumer Data Privacy Protection

Federal legislation that enacts a Consumer Privacy Bill of Rights should provide a national standard for protecting consumer data privacy where existing Federal data privacy statutes do not apply. Nationally uniform consumer data privacy rules are necessary to create certainty for companies and consistent protections for consumers. These rules should take into consideration the need for certain information to be available for law enforcement-related purposes. Moreover, national uniformity is crucial to preserving the incentives that the Administration's framework provides through the multistakeholder process. Stakeholders' incentives to participate in the multistakeholder process, and companies' incentives to adopt codes of conduct, would be diminished if States enacted laws with more stringent requirements. The Administration therefore recommends that Congress preempt State laws to the extent they are inconsistent with the Consumer Privacy Bill of Rights as enacted and applied. The Administration also recommends that Congress provide forbearance from enforcement of State laws against companies that adopt and comply with FTC-approved codes of conduct.[16]

Additionally, the Congressional Research Service has a list of various bills that have been submitted to Congress, and have been re-submitted regarding information privacy protections.[17] Anyone considering voting for this topic area should really take the time to read this report.[18] There have been numerous Congressional hearings on the topic area, yet little legislation has actually passed. For the purposes of policy debate, this provides students with a strong literature base on both sides of the question while still upholding the minimal standards of inherency, harms and solvency.

Alternatively, in 2002, Professor Solove wrote:

I advocate access and use restrictions on information as well as a federal baseline of protection for all public records beyond the limited scope of DPPA. The key issue is whether such a solution would be constitutional. As long as access and use restrictions are based on a conditional grant of access, they will pass constitutional muster. Further,

> the Constitution establishes an obligation to protect against disclosure and uses of information by the government. Today, government public record systems are not meeting this constitutional obligation. States must begin to rethink their public record regimes, and the federal government should step in to serve as the most efficient mechanism to achieve this goal. It is time for the public records laws of this country to mature to meet the problems of the Information Age.[19]

In 2006, Solove and Hoofnagle detailed a "Model Regime for Privacy Protection."[20] This is a plan to update the 1974 Privacy Act, a law that has not been substantially updated in over 30 years. They conclude, "There must be a meaningful regulation that limits the collection of personal data, lists acceptable uses, guarantees accuracy, provides security, and restricts retention of personal information by government agencies, especially since they are acquiring more and more data about individuals."[21]

Duke University Law Professor, Sarah Ludington, provides two possible solvency mechanisms. First, the creation through common-law (i.e. Supreme Court precedent) of a new tort; and second comprehensive federal legislation regarding data mining:

> It is again time to propose a tort for the misuse of personal information. The new tort will borrow from existing areas of law-- the four privacy torts and existing privacy statutes--but will be tailored to address the specifics of information abuse. Seen in the context of existing privacy torts and statutes, the tort is not a radical departure from the existing scheme, but more of a gap-filler or a cautious expansion, as it addresses injuries that implicate core privacy interests but currently have no remedy. Like the appropriation tort, the new tort remedies the harm to an individual caused by his loss of control over his identity when a data trader uses it without his permission. Like the Privacy Act, the new tort uses the principles of Fair Information Practices--notice, choice, access, and security --as the minimum standard for acceptable data management. The tort charts new ground in expanding the definition of what is considered private, in targeting commercial uses of data, and in transferring the principles of Fair Information Practices from the public sector to the private sector. This is what the tort would look like:
> • One who collects, stores, analyzes, or trades in personal information is liable to the subject of that information for the failure to use Fair Information Practices.
> • The tort would apply to any private entity that collects, stores, analyzes, or trades in personal information.
> • Personal information would include any information that is linked with an individual.
> • The tort would impose on data traders a duty to use Fair Information Practices (based on the principles of notice, choice, access, and security).
> • The tort would protect the individual's privacy interests in choice and control--choice about who may receive his personal information and control over the information revealed and how the recipient may use it. Accordingly, damages would be awarded based on injuries to the individual's choice and control.

[Ellipsis of several pages]

> The most positive effect of a new tort would be the creation of an incentive for data traders to invest in better data security technologies and to take seriously their obligation to use Fair Information Practices. A viable personal information tort would force data traders to implement better systems of obtaining consumer consent to the collection and use of their personal information. After a few successful lawsuits for the misuse of personal information, data traders would realize that they must obtain consent for data processing, requiring them to discover the privacy preferences of their data subjects and motivating them to seek a self-imposed solution.
> Ironically, a patchwork of common law tort regimes may have data traders begging for comprehensive federal legislation. Ultimately, sweeping federal legislation will be the most effective way to rein in the data traders, given the portability of data, the pervasiveness of the current problems, and the inevitability that misuses will increase as data technology grows ever more sophisticated. However, even an imperfect common law claim may provide a small foothold on a remedy for individuals who have been harmed but currently have no recourse to redress that harm. And, as the history of employment discrimination litigation shows, that legislation will be better constructed if it is built on the experience of the common law (footnotes removed).[22]

Professor Kang has an entire draft federal law proposed in his 1998 Stanford Law Review article. The proposal is the "Cyberspace Privacy Act."[23] An even more innovative approach to solving information privacy issues has been advanced by Lang, et. al. in March, 2012:

> Mandatory laws prohibiting or limiting self-surveillance seem exceedingly unwieldy and unlikely. After all, in modern American culture, how feasible is it for the government to say that you cannot measure yourself? Another predictable response is to suggest some technological fix, which typically touts encryption and efficient individual-preference expression. But so-called privacy-enhancing technologies by themselves--without supporting structures--have historically failed. Finally, there will be those who argue in favor of self-regulation although that means embracing the status quo and its predictable privacy displacement. We suggest a novel structural strategy: We call forth the Personal Data Guardians ("PDGs"). A. Personal Data Guardian. Our strategy is to introduce into the information ecosystem a new species, which functions as a professional intermediary between the individual client and those who would process the client's self-surveillance data. Specifically, we seek to jumpstart the creation of the PDG, whose principal mission is to maintain a digital storage locker called a Personal Data Vault ("PDV"). An individual client would upload her Personal Data Stream into that PDV, maintained by her PDG, instead of into some amorphous cloud owned and operated by some faceless third party.
> 1. Role Ideology. The PDG would embrace a professional identity of expertise and service, as has been done by other professionals such as lawyers, accountants, financial planners, and librarians. Their role ideology would include the core idea of acting as trustworthy confidantes on behalf of their clients (vis-à-vis third-party snoops, subpoenas, and government surveillance), zealous advocates who negotiate for best informational terms vis-à-vis third-party application service providers (3P-ASPs), and wise counselors to their individual clients about their decisions regarding self-surveillance data.

2. Professional Self-Regulation

The PDG would be an individual human being, licensed as a professional by a state self-regulatory body, which would be most easily created by state statute. This professional association would adopt minimum standards to enter into the profession, which could include infrastructural capacity as well as technological, legal, and business competence, and minimum requirements of continuing education. The association would also adopt internal model rules of ethical and professional behavior, whose violation could lead to enforcement actions by the disciplinary arm of the association as well as malpractice suits by clients. Following the analogy with lawyers, PDGs could partner with other Guardians to create a firm--in a general partnership or in a limited liability partnership.[24]

….

In privacy debates, any new problem is often met by calls for direct regulation or laissez faire trust of the market. Our approach seeks a novel path between the two. Instead of direct behavioral regulation or blind faith in the market, our strategy is to modify indirectly the information ecosystem by introducing a new species, the PDG. This new creature would be a faithful agent to its client and would store self-surveillance data in its PDV. The PDG would also act as a professional intermediary with third parties who seek access to such data.

Although we have painted with broad strokes, we believe that the PDG framework is a viable, concrete solution to the problem of self-surveillance. What is more, if the PDGs come to be, they will themselves become invested stakeholders, able to shape and alter future privacy policies in this and other domains. Indeed, if the framework functions well in this context, it could be expanded incrementally to help solve adjacent or related privacy problems.[25]

Professor Hirsch uses the development of Environmental Protection laws as a model for the creation of new information privacy protection legislation:

Second generation strategies appear well suited to privacy protection in the digital economy. As was mentioned above, privacy injuries, while costly, are seldom "toxic," so strict accountability may not be as critical. On the other hand, the cost of regulation looms larger here. Second generation strategies, which draw on firms' ingenuity in coming up with low-cost solutions, should prove less costly. They should also be more able to adapt to the rapid innovation and technological change that characterizes information-based businesses. Finally, widespread industry and public sentiment against government intervention in the digital economy may make second generation strategies more politically feasible than command-and-control regulations. The environmental experience suggests that second generation regulatory strategies hold the most potential for the digital economy.

Four of these second generation environmental regulatory methods show special promise for the protection of privacy. Regulators could apply an emission fee approach to the problem of spam. Further, the government could adapt regulatory covenants, pollution

release and transfer registers, and government promotion of environmental management systems for use in enhancing informational privacy.[26]

…

AN EMISSION FEE SYSTEM FOR SPAM

Government could implement an emission fee system for reducing spam by charging a fee per email sent. The fee should be equivalent to the damage that the spam email causes. This can be measured as a function of the time spent deleting the message, the cost of filters used to capture it, the inconvenience caused by the loss of improperly filtered or deleted emails, and the payment of higher fees for Internet service. Additional research will be required to determine what this amount should be. For the present purposes, assume that the fee is one-tenth of a cent per email. A spammer sending one million messages a day would now have to pay $1,000 per day, or $365,000 per year, for a privilege that previously had been far less expensive. This could give them an incentive to better target their products to individuals who might actually be interested in them. Internet marketers who figured out targeting methods that cost less than the price of the fee would gain an advantage over competitors who did not. The more they narrowed their email distribution, the greater this competitive advantage would grow. This fee should drive socially beneficial innovation. It should also cause a weeding out of the email messages with the smallest value to recipients in favor of those with the most, because the senders of the latter would get a greater return and be more able to bear the fee. The email fee system would accordingly lead to more efficient allocation of inbox space. The closest analogy from the environmental field would be "congestion fee" systems that operate to reduce traffic congestion during peak commuting periods. These systems charge an extra fee for using busy roads during the traditional morning and evening commuting times. They seek to impose on the driver the "significant negative externalities she imposes upon society in the form of slowing down other motorists, poorer air quality, added noise, and wasted fuel resulting from idling," and thereby cause some to shift to mass transit, carpooling, or other practices that minimize these externalities. The email fee system would be similar although it would alleviate inbox, rather than highway, congestion.

…

The covenanting approach could be used to protect informational privacy. Just as the Dutch government was getting ready to regulate CO2 emissions, the federal government is now considering actions to protect informational privacy. This should give information-intensive industries a reason to seek a deal. The existence of respected privacy advocacy groups that might add ideas and credibility to the negotiation also augurs well. The conditions are right for the federal government to sit down with the industries that collect and use personal information and to negotiate protective measures that are also workable for business.

…

> Another second generation environmental strategy-Pollution Release and Transfer Registers (PRTRs)-would also serve as a useful model for privacy protection. PRTRs inform the public about pollution releases from specific facilities, thereby giving these organizations an incentive to pollute less. For example, the Emergency Planning and Community Right to Know Act (EPCRA) requires companies annually to report the quantity of hazardous chemicals that they have released into the environment or transferred off-site. EPA incorporates this information into the Toxic Release Inventory (TRI), a national computerized database that is available to the public over the Web, and issues an annual report naming those facilities that have released the most toxic substances. No company wants to be near the top of this list. Publication of the TRI accordingly creates a strong incentive for businesses to reduce their toxic releases and "ha [s] been credited with stimulating a dramatic reduction in on-site inventories and releases of toxic chemicals." Between 1988 and 1998, toxic releases reported on the TRI decreased by 45.3%. Notably, TRI achieved this result without issuing a single, substantive requirement. Instead, it used information disclosure to encourage companies to come up with their own ways of improving environmental performance. In this sense, PRTRs are very much a second generation strategy.

…

> Just as an EMS improves environmental performance, a privacy-focused analogue-call it a Personal Information Management System (PIMS)-could protect informational privacy. The typical privacy officer, much like the traditional environmental manager, is compartmentalized in the privacy "box" and is often unable to affect the core, strategic decisions that are at the root of the company's privacy impacts. A PIMS would connect the privacy officer to other employees in the organization and allow her to work with them to improve the company's privacy performance. It would make her less of an internal compliance officer, who spends the day getting others to meet legal requirements, and more of a manager of others' privacy-related actions. This is what the CPO of the Fortune 500 company was trying to achieve when she adapted her firm's EMS for privacy purposes.

…

> Although command-and-control regulation is not the best fit for the information economy, we should not give up on government action to protect privacy. To the contrary, the information economy needs such initiatives. Without them, a tragedy of the commons threatens email, e-commerce, and other online activity. To borrow one final environmental analogy, regulators need to develop strategies that will allow for the "sustainable development" of the information economy. Such policies will support innovation and prosperity but will do so in a way that sustains the personal privacy on which the digital economy itself depends. Second generation environmental laws and policies offer valuable lessons for the design of this new regulatory framework and for the protection of privacy in the Information Age.

Regarding Health information, one author has proposed the following:

Examples of security standards and guidelines already exist in some sectors, but they are not widely applied in health research. For instance, the National Institute of Standards and Technology has developed standards and guidance for the implementation of the Federal Information Security Management Act of 2002, which was meant to bolster computer and network security within the federal government and affiliated parties (e.g., government contractors). These include standards for minimum security requirements for information and information systems, as well as guidance for assessing and selecting appropriate security controls for information systems, for determining security control effectiveness, and for certifying and accrediting information systems (NIST, 2007). However, two recent GAO reports found that although the federal government is improving information security performance, a number of significant information security control deficiencies remain (GAO, 2008a). HHS, working through its Office of the National Coordinator for Health Information Technology,[14] could play an important role in developing or adapting standards for health research applications, and then encourage and facilitate broader use of such standards in the health research community.[27]

…

In addition, the federal government should support the development and use of:

- Genuine privacy-enhancing techniques that minimize or eliminate the collection of personally identifiable data.
- Standardized self-evaluations and security audits and certification programs to help institutions achieve the goal of safeguarding the security of personal health data.

Effective health privacy protections require effective data security measures. The HIPAA Security Rule (which entails a set of regulatory provisions separate from the Privacy Rule) already sets a floor for data security standards within covered entities, but not all institutions that conduct health research are subject to HIPAA regulations. Also, the survey data presented in this chapter show that neither the HIPAA Privacy Rule nor the HIPAA Security Rule have directly improved public confidence that personal health information will be kept confidential. Therefore, all institutions conducting health research should undertake measures to strengthen data protections. For example, given the recent spate of lost or stolen laptops containing patient health information, encryption should be required for all laptops and removable media containing such data. However, in general, given the differences among the missions and activities of institutions in the health research community, some flexibility in the implementation of specific security measures will be necessary.

Enhanced security would reduce the risk of data theft and reinforce the public's trust in the research community by diminishing anxiety about the potential for unintentional disclosure of information. The publication of best practices and outreach to all stakeholders by HHS, combined with a cooperative approach to compliance with security standards, such as self-evaluation and audit programs, would promote progress in this

area. Research sponsors could also play a role in fostering the adoption of best practices in data security.[28]

Affirmative Advantage Areas in no particular order:

Right to Privacy Good

> "The humiliation, economic harm and discrimination suffered by these people raise serious questions about the impact of information technologies on personal autonomy, social relationships, and democracy. Sociologist David Lyon argues that surveillance enables a type of "social sorting" where computer code is used to classify groups of people in "ways that tend to reinforce social divisions." Parliamentarian John Godfrey reminds us that a loss of privacy chills the exercise of other human rights, like freedom of speech or freedom of assembly. Alan Westin contends that, if privacy is going to survive in the technological age, individuals, groups and institutions must be able to determine for themselves, when, how and to what extent information about them is communicated to others."[29]

Dehumanization

Autonomy[30]

Employment Discrimination

Insurance Discrimination

Healthcare Discrimination[31]

Genetic Privacy (see also, "Gattica")[32]

Orwell was right, but forgot about Corporations as the New Big Brother

Biopower/State of Exception—that's right Foucault and Agamben become topical advantages

Biometrics[33],[34]

Human Rights Credibility

Internet Global leadership

Internet Global Cooperation/interoperability[35]

Increase Consumer Confidence[36]

Increase Economic Growth[37]

Revolutionary power

Sovereignty Bad/Good

Abortion Rights (very limited) only that information regarding the medical procedure could not be used against a person for the purpose of prosecution (has inherency problems because abortion is still legal).

Internet leads to global consciousness

Global movements

Technology Innovation good

More advantage areas can be found in the Privacy Rights Clearinghouse website/[38]

Negative Ground:

First, negative teams would actually have uniqueness on this topic because there is really inherency. That is a substantial change from the Middle East topic debacle. But, for those requiring a list negative arguments, here we go:

Counterplans:

States Counterplan

Agent Counterplans

Regulation Negotiation Counterplans

WTO Counterplans

Consult Counterplans

Disadvantages:

Politics (we will always have politics)

Elections (at least until November)

Business Confidence (this should be a great debate between the affirmative arguing link turns based on consumer confidence and stability versus negatives arguing that the new business models rely on obtaining consumer data)[39]

Privacy bad/Rights Malthus

Human Rights Leadership leads to pressure on Russia, China, Iran, etc.

Relations disads with countries having differing views on the extent of privacy protections

WTO credibility

Agreements with the EU

Economy Good/Bad

Cyberterrorism/sabotage[40]

Terrorism

Espionage

Pathological periods---expanding rights is bad, leads to a roll-back.

Disease/Pandemics

Collapse of the Healthcare System

Kritik Ground:

Cap! We will always have the Cap K! Yes, you get your Cap K/Neoliberalism K links. The Obama Proposal, for example, states specifically that the failure to protect consumer privacy reduces the number of people willing to participate in the global internet economy.[41] I am sure Zizek has shat out something about how the internet and informational privacy stops the spread of socialism.

Racism/Gender. There is plenty of material out there about the digital divide.

Agamben/Foucault. This should typically be affirmative ground on this topic. However, the negative could spin links regarding reliance on the State to define what is and is not protected information only reifies the State, or creates new states of exception.

Privacy is bad.

Identifying the Right to Privacy is bad.[42]

Schlag

Baudrillard probably has something to say about the internet as hyperreality. Heidegger…" well, you said internet, and the internet is a form of technology, so….."

---

[1] Kang, J. 50 STNLR 1193, Stanford Law Review, INFORMATION PRIVACY IN CYBERSPACE TRANSACTIONS April, 1998.

[2]Samuel D. Warren and Louis D. Brandeis , 4 HVLR 193, Harvard Law Review THE RIGHT TO PRIVACY (1890)

[3] Id.

[4]Daniel J. Solove, 86 MNLR 1137, Minnesota Law Review ACCESS AND AGGREGATION: PUBLIC RECORDS, PRIVACY AND THE CONSTITUTION, June, 2002

[5] Id. See also, Jacqueline D. Lipton, Mapping Online Privacy, 140 N.W. U. L Rev. 477, 481-82 (2010)

[6] M. Joseph Kapkovic 5 CRITCSJ 1 The Crit: a Critical Studies Journal, OUR WALLS IN THE INFORMATION AGE, Spring, 2012

[7] http://www.media-awareness.ca/english/issues/privacy/us_legislation_privacy.cfm

[8] http://www.privacyrights.org/ar/Privacy-IssuesList.htm

[9] http://www.fas.org/sgp/crs/misc/R41756.pdf; "There is no comprehensive federal privacy statute that protects personal information. Instead, a patchwork of federal laws and regulations govern the collection and disclosure of personal information and has been addressed by Congress on a sector-by-sector basis. Federal laws and regulations extend protection to consumer credit reports, electronic communications, federal agency records, education records, bank records, cable subscriber information, video rental records, motor vehicle records, health information, telecommunications subscriber information, children's online information, and customer financial information. Some contend that this patchwork of laws and regulations is insufficient to meet the demands of today's technology."

[10] Dennis D. Hirsch, Georgia Law Review Fall, 2006, PROTECTING THE INNER ENVIRONMENT: WHAT PRIVACY REGULATION CAN LEARN FROM ENVIRONMENTAL LAW.

[11] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[12] Id.

[13] Id.

[14] Id.

[15] Id.

[16] Id.

[17] http://www.fas.org/sgp/crs/misc/R41756.pdf. See pages 3-4.

[18] http://www.fas.org/sgp/crs/misc/R41756.pdf.

[19] Daniel J. Solove, 86 MNLR 1137, Minnesota Law Review ACCESS AND AGGREGATION: PUBLIC RECORDS, PRIVACY AND THE CONSTITUTION June, 2002

[20] Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. OF ILL. L. REV. 357, 357 (2006). See also, Rachel Greenstadt, 2005 http://infosecon.net/workshop/pdf/48.pdf : "Adhering to the theory of second best government

regulation seems the most feasible interim approach. While governments may not be truly disinterested third parties, every model requires or directly benefits from some amount of government regulation. There doesn't seem to be any better place to start."

[21] Id.

[22] Sarah Ludington, 66 MDLR 140**,** Maryland Law Review REINING IN THE DATA TRADERS: A TORT FOR THE MISUSE OF PERSONAL INFORMATION.

[23] Jerry Kang, 50 STNLR 1193, Stanford Law Review, INFORMATION PRIVACY IN CYBERSPACE TRANSACTIONS April, 1998; see Appendix "A."

[24] Jerry Kang, Katie Shilton, Deborah Estrin, Jeff Burke, Mark Hansen, 97 IALR 809 Iowa Law Review SELF-SURVEILLANCE PRIVACY, March, 2012

[25] Id.

[26] Dennis D. Hirsch, Georgia Law Review Fall, 2006, PROTECTING THE INNER ENVIRONMENT: WHAT PRIVACY REGULATION CAN LEARN FROM ENVIRONMENTAL LAW

[27] http://www.ncbi.nlm.nih.gov/books/NBK9579/

[28] http://www.ncbi.nlm.nih.gov/books/NBK9579/

[29] http://www.media-awareness.ca/english/issues/privacy/why_issue_privacy.cfm

[30] http://www.ncbi.nlm.nih.gov/books/NBK9579/

[31] http://www.ncbi.nlm.nih.gov/books/NBK9579/

[32] http://www.ncbi.nlm.nih.gov/books/NBK9579/

[33] Ann Cavoukian and Alex Stoianov, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security and Privacy* (http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf).

[34] http://www.bioprivacy.org/privacy_fears.htm

[35] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[36] Id.

[37] http://www.fas.org/sgp/crs/misc/R41756.pdf "Stakeholders routinely acknowledge that the continued success of electronic commerce depends upon the resolution of issues related to the privacy and security of online personal information. The U.S. Department of Commerce recently reiterated that the large-scale collection, analysis, and storage of personal information is central to the Internet economy; and that regulation of online personal information must not impede commerce."

[38] http://www.privacyrights.org/ar/Privacy-IssuesList.htm

[39] http://www.fas.org/sgp/crs/misc/R41756.pdf "Behavioral advertising, a form of online advertising, is delivered based on consumer preferences or interest as inferred from data about online activities. In 2010, over $22 billion was spent on online advertising.4 This revenue allows websites to offer content and services for free. What They Know, an in-depth investigative series by the Wall Street Journal, found that one of the fastest growing Internet business models is of data-gatherers engaged in "intensive surveillance of people [visiting websites] to sell data about, and predictions of, their interests and activities, in real time."

[40] http://www.mttlr.org/volnine/cate.pdf

[41] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[42] http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf