2005

A Model Regime of Privacy Protection (Version 1.1)

Daniel J. Solove
George Washington University Law School, dsolove@law.gwu.edu

Chris Jay Hoofnagle

A MODEL REGIME OF PRIVACY PROTECTION
Version 1.1

by
Daniel J. Solove[1] & Chris Jay Hoofnagle[2]

March 10, 2005

NOTE: We have issued a revised and updated version of this paper incorporating comments received on this draft.

You can download Version 2.0 at:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=699701

Privacy protection in the United States has often been criticized, but critics have too infrequently suggested specific proposals for reform. Recently, there has been significant legislative interest at both the federal and state levels in addressing the privacy of personal information. This was sparked when ChoicePoint, one of the largest data brokers in the United States with records on almost every adult American citizen, sold data on about 145,000 people to fraudulent businesses set up by identity thieves.

In the aftermath of the ChoicePoint debacle, both of us have been asked by Congressional legislative staffers, state legislative policymakers, journalists, academics, and others about what specifically should be done to better regulate information privacy. In response to these questions, we believe that it is imperative to have a discussion of concrete legislative solutions to privacy problems.

What appears below is our attempt at such an endeavor. Privacy experts have long suggested that information collection be consistent with Fair Information Practices. This Model Regime incorporates many of those practices and applies them specifically to the context of commercial data brokers such as Choicepoint. We hope that this will provide useful guidance to legislators and policymakers in crafting laws and regulations. We also intend this to be a work-in-progress in which we collaborate with others. We welcome input from other academics, policymakers, journalists, and experts as well as from the industries and businesses that will be subject to the regulations we propose. We invite criticisms and constructive suggestions, and we will update this Model Regime to incorporate the comments we find most helpful and illuminating. We also aim discuss some of the comments we receive in a "commentary" section. To the extent to

---

[1] Associate Professor of Law, George Washington University Law School; JD Yale. Professor Solove has discussed many of the problems and solutions herein in his book, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004).

[2] Director, Electronic Privacy Information Center West Coast Office; JD U. GA. Chris Hoofnagle has discussed many of the problems and solutions herein in his articles, *Big Brother's Little Helpers*, http://ssrn.com/abstract=582302; and *Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors*, http://ssrn.com/abstract=679581.

which we incorporate suggestions and commentary, and if those making suggestions want to be identified, we will graciously acknowledge those assisting in our endeavor.[3]

Daniel J. Solove
dsolove@law.gwu.edu

Chris Jay Hoofnagle
hoofnagle@epic.org

TABLE OF CONTENTS

[3] Marc Rotenberg of the Electronic Privacy Information Center and Beth Givens of the Privacy Rights Clearinghouse have provided substantial comments which are incorporated in Version 1.1.

NOTICE, CONSENT, CONTROL, AND ACCESS

1. Universal Notice

(a) Problem

There is no general knowledge about the companies using personal information. In order to grant consent, gain access, or otherwise exercise one's rights with regard to personal information maintained by data brokers, credit reporting agencies, and other institutions, people must know about what institutions are collecting their data. Providing such rights without knowledge of the companies will be meaningless. For example, in the ChoicePoint security scandal, most people had no idea that ChoicePoint existed let alone that it was collecting and selling their personal data. Moreover, as the ChoicePoint security scandal demonstrates, data brokers routinely sell personal information with little oversight about who may receive the data and how it will be used. The problems of such a system were emphatically illustrated in *Remsburg v. Docusearch*, 149 N.H. 148 (2003), where a data broker was employed by a stalker to locate and murder Amy Boyer. ChoicePoint has repeatedly invited a national debate and discussion about data brokers, but such a discussion cannot meaningfully take place unless people are informed about what information data brokers have and what they do with that information.

(b) Legislative Mandate

To ensure meaningful access, opt-out, and other rights, there must be a way to provide people with notice about all of the companies collecting their information.

(c) Specific Solution

Any company primarily engaged in interstate collection, maintenance, and/or sale of personally identifiable information shall register with the FTC. Such registration shall include the nature of personal information collected, , the name and contact information for the data controller, as well as a clear and concrete description of the uses to which the information is put. Data brokers shall also disclose the types of businesses and entities to whom they disclose personal information as well as what safeguards they have in place for vetting those entities that receive the data. This information shall be publicly disclosed by the FTC on a website.

2. Meaningful Informed Consent

(a) Problem

Many data transfers and uses by companies occur without the meaningful informed consent of consumers. The current regime of allowing consumers to opt-out of data sharing, as embodied in the Gramm-Leach-Bliley Act, is ineffective. The incentives are such that companies benefit if they make opting out as cumbersome as possible and do not adequately inform people about the uses of their data. As a result, very few people opt-out, and those who try find the process difficult and time-consuming. There are, of course, many uses of information for which people

would readily agree to. However, people are often provided an all-or-nothing choice – surrender total control of information or be denied useful services or uses of information that they desire.

(b) Legislative Mandate

There must be a way to ensure that consumers can exercise meaningful informed consent about the uses and dissemination of their personal information.

(c) Specific Solution

Companies that collect personal information should be required to first obtain an individual's consent before using it for an unrelated secondary use, except for the investigation of fraud. To the extent that companies endeavor to use personal information for secondary uses without first obtaining individual consent, such uses shall be specifically authorized by statute or regulation. For all new uses of personal information, companies must either be authorized by statute to engage in such a use or seek the consent of the individuals to whom the information pertains. When a company engages in any new use authorized by statute, it shall disclose such expansion in use immediately to the FTC and the change shall be displayed clearly on the FTC website so that individuals are aware of the change.

3. One-Step Exercise of Rights

(a) Problem

There are hundreds, possibly thousands, of companies that collect and trade in personal information. To the extent that the law provides people with rights of access, opt-in, opt-out, limitation of use and transfer, and so on, these rights must currently be exercised one-at-a-time at each individual company. For example, under the Gramm-Leach-Bliley Act, people have a right to opt-out of the transfer of their data to third parties for marketing purposes. Many people have dealings with a multitude of financial institutions, and opting out of each one can be onerous and time-consuming. When data brokers are brought into the fold, this will make such exercise of rights exponentially more difficult. Imagine the time it would take to opt-out with hundreds of different companies. And this example merely involves opt-out. There are many other rights that people exercise as well, and exercising all with the multitude of companies individually will prove nearly impossible and time-prohibitive.

(b) Legislative Mandate

To ensure the meaningful exercise of rights with regard to personal information, there must be a way to exercise these rights in an efficient and easy manner that is centralized.

(c) Specific Solution

In conjunction with the universal notice, the FTC shall develop a centralized mechanism for people to exercise their rights with respect to their personal information. Such a mechanism

would mimic the Do Not Call website, which allows individuals to opt-out of telemarketing and verify their enrollment by visiting a single website.

4. Individual Credit Management

(a) Problem

As the ChoicePoint snafu illustrates, individuals are not in control of the basic information that is used for credit identification authentication. Numerous individuals and companies can access people's credit information without that person's knowledge. Identity thieves take advantage of this system, as they can seek loans or credit cards with creditors, who will check the victim's credit without informing the victim. Such credit checks are often the beginning steps in an identity theft. Because these checks can occur without the victim's knowledge or consent, the identity thief can readily obtain credit in the victim's name surreptitiously. Many identity thefts would be stopped at their incipiency if only the victim had known about the access to the victim's credit records and could have blocked such access. Moreover, the problem exacerbates identity thefts after they are underway because victims are unaware that they have been victimized until months or years later.

(b) Legislative Mandate

To ensure effective individual management of credit reporting, there must be a way for individuals to have knowledge when entities attempt to access their credit records and have the ability to block such access.

(c) Specific Solution

First, notice shall be issued whenever any person or entity makes an inquiry on or accesses the credit report of another. The individual can choose to receive such notice by mail, telephone, or email. Second, unless individuals choose otherwise, credit records shall be "frozen," whereupon they can only be accessed by others after the individual has preapproved the release of such records.

5. Access to and Accuracy of Personal Information

(a) Problem

ChoicePoint and other data brokers collect detailed dossiers of personal information on practically every American citizen. Most people haven't even heard of these companies. Even if they do know about these companies, people have no way of knowing what information is maintained about them, why it is being kept, to whom it is being disseminated, and how it is being used. The records maintained by these companies can have inaccuracies. This wouldn't matter much if the information were never used for anything important. But the data is being used in ways that directly affect individuals – by businesses for background checks, creditors for assessing financial reputations, the government for law enforcement purposes, and private investigators for investigation.

(b) Legislative Mandate

There must be a way for individuals to ensure that their personal information maintained by various data brokers is maintained accurately.

(c) Specific Solution

Individuals shall, in a centralized manner, be able to access their information from data brokers at no cost. As with credit reporting agencies under the Fair Credit Reporting Act, a procedure shall be developed for individuals to correct inaccuracies in their records.

SECURITY OF PERSONAL INFORMATION

6. Secure Identification

(a) Problem

Businesses and financial institutions currently grant access to people's records when the accessor merely supplies a Social Security Number, date of birth, mother's maiden name, or other forms of personal information that is either available in public records or sold by data brokers. This makes the repositories of individuals' personal data and their accounts woefully insecure, as identity thieves can readily obtain the information needed to gain access and usurp control. As the ChoicePoint security scandal illustrates, Social Security Numbers and other personal information about hundreds of thousands of people can readily fall into the hands of identity thieves.

(b) Legislative Mandate

There must be a way to prevent readily available pieces of personal information from being used as passwords to gain access to people's records and accounts.

(c) Specific Solution

Companies shall develop methods of identification which (1) are not based on publicly available personal information or data that can readily be purchased from a data broker; and (2) can be easily changed if they fall into the wrong hands. Whereas Social Security Numbers cannot be changed without significant hassle, and dates of birth and mother's maiden names cannot be changed, identifiers such as passwords can be changed with ease. Furthermore, they are not universal, and thus a thief with a password cannot access all of a victim's accounts – only those with that password. Biometric identifiers present problems because they are impossible to change, and if they fall into the wrong hands could prove devastating for victims as well as present ongoing risks to national security. Therefore, passwords are a cheap and effective way to limit much identity theft and minimize the problems victims face in clearing up the damage caused by identity theft.

7. Disclosure of Security Breaches

(a) Problem

When companies suffer security breaches that result in personal information being leaked or falling into the hands of unauthorized third parties, the people to whom the personal information pertains are made more vulnerable to fraud and identity theft. They often are not aware of this, and are unable to take steps to protect themselves such as monitoring their credit reports. This was dramatically illustrated by the ChoicePoint security breach, which apparently was the second time where the company had sold personal information to criminals. The first incident occurred in 2002 and only recently came to public light because of California's information security breach disclosure requirements. ChoicePoint is not the only commercial data broker that has disclosed records to others improperly—in 2002 and 2003 two individuals were able to crack commercial data broker Acxiom's databases, leading to the release of 20 million names and Social Security Numbers.

(b) Legislative Mandate

There must be a way for individuals to learn about security breaches that result in the leakage or improper access of their personal data.

(c) Specific Solution

Companies shall be placed under an affirmative obligation to provide direct notice to the individuals whose data has been leaked or improperly accessed. Such a statute could be modeled on California's information security breach law, codified at Civil Code § 1798.29. Individuals should also receive a copy of the dossier or information given to the unauthorized party.

BUSINESS ACCESS TO AND USE OF PERSONAL INFORMATION

8. Social Security Number Use Limitation

(a) Problem

Numerous businesses and organizations demand that a person provide a Social Security Number and then use that number as a password for access to accounts and data. Many schools and other organizations use Social Security Numbers on identification cards, thus ensuring that when a wallet is lost or stolen, one's Social Security Number is exposed. The use of Social Security Numbers is so extensive that as simple a transaction as signing up for cell phone service often requires disclosing one's Social Security Number.

(b) Legislative Mandate

There must be a way to reduce the use of Social Security Numbers by private sector businesses.

(c) Specific Solution

Unless specifically authorized by statute or regulation, business and other privacy sector entities shall be barred from using Social Security Numbers for identification purposes. A useful starting point is the framework of protections for the Social Security Number embodied in California Civil Codes § 1785, 1798, and 1786.

9. Access and Use Restrictions for Public Records

(a) Problem

Public records were once scattered about the country, and finding out information on individuals involved trekking to or calling a series of different local offices. Today, massive database companies sweep up the data in public record systems and use it to construct dossiers on individuals for marketers, private investigators, and the government. This is what ChoicePoint does. These uses of public records turn the justification for public records on its head. Public records are essential for effective oversight of government activities, but commercial data brokers have perverted this principled purpose, and now public records have become a tool of businesses and the government to watch individuals.

(b) Legislative Mandate

There must be a way to regulate access and uses of public records that maximizes exposure of government activities and minimizes the disclosure of personal information about individuals.

(c) Specific Solution

Access to personal information in public records shall be restricted for certain purposes. For example, accessing public records to obtain data for commercial solicitation should be prohibited. Other purposes shall be permitted: monitoring the government, research, educational purposes, tracing property ownership, and other traditional non-commercial purposes. Data brokers obtaining such data should be required to promise via contract, in return for receiving such data, to be subject to reasonable use restrictions on that data and to demand that those to whom the data is transferred also restrict uses and transfers. Such regulation would have allowed for greater control over ChoicePoint's use of personal data, since it obtained a significant amount of its information from public records. Additionally, federal, state, and local agencies that maintain public record systems must make substantial efforts to limit the disclosure of Social Security Numbers, phone numbers, addresses, and dates of birth.

10. Curbing Excessive Uses of Background Checks

(a) Problem

Background checks are cheaper now than ever before, leading to a situation where individuals are being screened for even menial jobs. We risk altering our society to one where the individual can never escape a youthful indiscretion or a years-old arrest, even for a minor infraction. Background checks are frequently being used by employers even for jobs that do not involve

security-related functions, the handling of large sums of money, or the supervision of children or the elderly.

(b) Legislative Mandate

There must be a way to limit the use of background checks to those jobs where there is a reasonable and justifiable need.

(c) Specific Solution

Background checks should only be performed in contexts where fiduciary relationships are involved, where a large amount of money is handled, where employment involves care taking, or any of the jobs enumerated by the Employee Privacy Protection Act, 29 U.S.C. § 2007. Whether background checks are performed by employers or by companies hired to do the screening, the employee or prospective employee shall receive a copy of the actual investigation.

11. Private Investigators

(a) Problem

Private investigators routinely access personal information about individuals from data brokers. Private investigators often operate without the extensive regulation that public law enforcement officials must heed. In some states, they are not subject to licensure; in others they are subject only to a pro forma process. As a result, they can be a source of great abuses. The Rebecca Schaeffer incident that sparked the passage of the Drivers' Privacy Protection Act demonstrates the problem. A private investigator obtained actress Rebecca Schaeffer's home address from a state DMV office. The investigator was working for a stalker who used the information to go to Schaeffer's home and murder her. More recently, Amy Boyer was murdered by a stalker who had hired private investigators to locate her.

(b) Legislative Mandate

There must be a system that ensures greater accountability in the private investigator profession.

(c) Specific Solution

Each state should be required to establish minimum standards for licensure and oversight of the private investigator industry. Such standards should address the use of pretexting (pretending to be another person in order to gain access to someone's account or to gain information), establish a duty of care to those who are investigated, and prohibit the use of invasive practices, such as sorting through individuals' trash, employing electronic listening devices, etc.

GOVERNMENT ACCESS TO AND USE OF PERSONAL DATA

12. Limiting Government Access to Business and Financial Records

(a) Problem

Increasingly, the government is gathering personal information from businesses and financial institutions. Companies such as ChoicePoint have multi-million dollar contracts with government agencies to supply them with personal information. The Fourth Amendment is often inapplicable because in a series of cases, including *United States v. Miller,* 425 US 435 (1976) and *Smith v. Maryland,* 442 US 735 (1979), the Court has held that whenever a third party possesses personal information, there is no reasonable expectation of privacy. In the Information Age, it is impossible to live without extensive information about one's life existing in the hands of various third parties: phone companies, cable companies, Internet Service Providers, merchants, booksellers, employers, landlords, and so on. Thus, the government can increasingly obtain detailed information about a person without ever entering her home

(b) Legislative Mandate

There must be a way to engage in electronic commerce and routine transactions without losing one's expectation of privacy in personal data.

(c) Specific Solution

Whenever the government attempts to access personal information from third parties that maintain record systems of personal information (databases or other records of personally identifiable information on more than one individual), the government should be required to obtain a special court order that requires probable cause and particularized suspicion that the information sought involves evidence of a crime. Exceptions should exist for reasonable law enforcement needs, including emergency circumstances.

13. Government Data Mining

(a) Problem

The government is increasingly researching, planning, and initiating data mining endeavors. Data mining entails combining and analyzing various records of personal information for suspicious patterns of behavior. This was envisioned on a grand scale with the Total Information Awareness project. Due to a public outcry, Congress nixed the program from the public budget. But a recent GAO report as well as the Technology and Privacy Advisory Committee report demonstrates that a number of government data mining programs are underway. Data mining threatens to undermine a longstanding Fourth Amendment principle, which holds that dragnet searches – those without prior particularized suspicion – are impermissible. Because there are serious inaccuracies in dossiers created by commercial data brokers, innocent people may be swept into these dragnets. Furthermore, the profiles and algorithms used to determine suspicious patterns of behavior are often kept secret, thus impeding public accountability or judicial

oversight, and providing no way to find out the extent of use of certain factors such as race, religion, and First Amendment activity.

(b) Legislative Mandate

There must be a way to ensure that government data mining does not permit law enforcement to engage in dragnet searches for prospective crimes. Where data mining is employed, it should occur in as open a way as possible with adequate judicial oversight and public accountability.

(c) Specific Solution

Subject to judicial oversight and normal search warrant requirements, prospective subject-based data mining should be permitted. Subject-based data mining involves analyzing records where a specific individual or individuals are identified and where there is particularized suspicion that they are involved in criminal activity. Pattern-based data mining presents greater difficulties. Prospective pattern-based data mining involves analyzing record systems for various suspicious patterns of activity and then investigating those individuals who meet the particular pattern or profile. Pattern-based data mining should be generally prohibited, as it involves a dragnet search. However, with appropriate judicial supervision and with a way to preserve the principle of particularized suspicion, pattern-based data mining should be permitted in cases where there are specific and articulable facts that a particular crime will or has occurred, that a particular limited type of record system (not a broad dossier) has information that is necessary to the investigation (no alternatives available), and where the inquiry into the record system is limited. Data mining profiles must be approved by a court prior to use and must be revealed to the public once the investigation is over. Moreover, as is currently done with wiretapping, government agencies engaging in data mining shall produce annual public reports to Congress describing the frequency and nature of their data mining activities.

14. Control of Government Maintenance of Personal Information

(a) Problem

The Privacy Act of 1974 is riddled with loopholes. Despite a requirement that government agencies disclose new record systems, they can readily avert other substantive requirements simply by declaring that they want to exempt these records. For instance, in 2003, the Justice Department administratively discharged the FBI of its statutory duty to ensure the accuracy and completeness of the over 39 million criminal records it maintains in its National Crime Information Center (NCIC) database. That database provides over 80,000 law enforcement agencies with access to data on wanted persons, missing persons, gang members, as well as information about stolen cars, boats, and other information. Aside from agencies exempting themselves from the requirements of the act, agencies have also employed the "routine use" exemption in such a broad fashion that it contravenes the intent of the Privacy Act.

(b) Legislative Mandate

There must be meaningful regulation limiting the collection of personal data, acceptable uses, accuracy, security, and retention of personal information by government agencies, especially since they are acquiring more and more data about individuals.

(c) Specific Solution

The Privacy Act must be updated. Over thirty years have gone by without a major re-examination of the Privacy Act, and one is sorely needed. Congress should empanel a new Privacy Protection Study Committee to examine government use of personal information comprehensively and make recommendations for legislation to update the Privacy Act. Specific changes shall include, but shall not be limited to: limiting the routine use exception, addressing the outsourcing of personal information processing to private sector businesses, strengthening the enforcement provisions of the Act, and overturning *Doe v. Chao***,** 124 S. Ct. 1204 (2004), so that violations of the Act are remedied by minimum damages provisions.

PRIVACY INNOVATION AND ENFORCEMENT

15. Preserving the Innovative Role of the States

(a) Problem

The recently enacted amendments to the Fair Credit Reporting Act preempted more protective state laws. As a result, states are less able to pass effective identity theft and privacy protections.

(b) Legislative Mandate

The ability of states to innovate new approaches to privacy protections must be preserved.

(c) Specific Solution

Most privacy protections in America have been created by state legislatures. The security breach law that resulted in ChoicePoint disclosing the recent sale of personal information to criminals was developed in California. Many of the most important protections in the Fair Credit Reporting Act originated in the states. Indeed, as Justice Brandeis once noted, "It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country." *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting). Legislation crafted to address privacy problems should only employ "floor preemption," thereby allowing states to innovate more comprehensive protections for individual rights.

16. Effective Enforcement of Privacy Rights

(a) Problem

Often, privacy rights are difficult to enforce. In many instances, it is difficult for victims to establish damages or causation when leaks or improper uses of their personal information result in identity theft or other harms. When a company discloses a person's data or violates its privacy policy by wrongfully transferring data to other companies or not providing adequate security, it is often difficult to prove actual damages. As a result, companies often lack sufficient accountability and sanctions when they engage in wrongdoing. About half of identity theft victims cannot tell how their personal information was even accessed, and thus do not know what parties should be pursued legally. Moreover, it is very difficult for identity theft victims to prove actual monetary damages even though they have spent considerable time fixing the harm and suffered great mental distress. With the ChoicePoint security debacle, people's personal information was sold to identity thieves. Although many did not suffer from identity theft, they still suffered harm, as they are now much more vulnerable to identity theft, have considerable mental unease, and must spend significantly more time monitoring their credit and accounts over a period that could last years.

(b) Legislative Mandate

There must be a way to ensure that privacy protections are enforced with meaningful sanctions as well as provide meaningful redress to victims.

(c) Specific Solution

There should be minimum liquidated damages provisions for companies that violate their privacy policies or that suffer a security breach due to negligence. Statutes must provide for individual redress. In the event of leaked information, the most effective way to address the problem in a way that avoids extensive class action litigation is to authorize state attorneys general to fine companies and establish a fund where victims can make claims for disbursements.

COMMENTARY

This section will be developed in subsequent versions as we receive comments and feedback.