Introduction
This topic deals with issues about who should control use of factual data that can be linked with identifiable persons. It focuses on the handling of transactional data – information created or exchanged within a voluntary transaction between two (or more) parties. It excludes traditionally confidential relationships (e.g., doctor-patient, lawyer-client). The question addressed is to what extent do modern laws on data privacy and data security threaten adverse impacts on ordinary transactional relationships.

The issues addressed here fall within the scope of modern debate about “privacy” and “data security” law. A premise in the privacy-activist community is that enhancements of privacy rights are needed and that protecting those rights requires expanded regulation with respect to transactional data. I plan to present instead a perspective that argues for allowing the evolution of markets, contract and related law that center on voluntarily undertaken obligations, while permitting regulation only in extreme cases.

The Language of Data Control
One manifestation of the information age is an increasing attentiveness to the importance of information as a source of value and thus a focus for legal and social policy debate. That attentiveness explains in part the emergence of “privacy” as an important issue during the past two decades. Privacy and data control themes focus on the relationship of multiple parties to control of data related to individuals. Despite similarities at this level, “privacy” and “data control” are separated by a vast gulf that defines theories aimed at entirely different policy issues.

In 1888, in a leading treatise on torts, Judge Thomas Cooley described privacy as the “right to be left alone.” 1 This phrase, which was repeated two years later in a famous article by Brandeis and Warren, 2 captures the essence of what has traditionally been the concept of “privacy” in this country. “Privacy” centers on a right to be free from unwarranted intrusions and from undesired disclosure of otherwise confidential facts about an individual. It is a right to keep things, places, and information away from third parties and from the public at large.

Privacy, in this coloration, thus refers to truly private or confidential information and places. Thus, privacy torts protect, albeit narrowly, against intrusive conduct engaged in by one party with respect to private facts or conduct related to another person. In addition, especially with respect to governmental acquisition of data, courts focus on the scope of governmental search and seizure activities, wiretap or other similarly intrusive conduct. In these contexts, there are two themes: 1) whether the person claiming a wrongful intrusion or disclosure had a reasonable expectation of privacy with respect to the information or place, and 2) whether wrongful disclosure would be highly embarrassing to a reasonable person. These themes, augmented by various other considerations, define the law of privacy.

But “privacy” in this sense is not what activists today mean when they assert the need to protect “privacy” rights in transactional data. Indeed, transactional data, by its nature, is not private. It has been voluntarily disclosed in, or created by, interactions with

another person or entity, rather than obtained through a wrongful intrusion.³ Even though “private” information is included within the umbrella of “data control” arguments, data control issues relate primarily to information that is not secret, private or confidential (e.g., a person’s name, age, etc.), nor embarrassing in nature.

Arguments that use or disclosure of transactional data should be restricted propose that one party (data subject) should have a right to control the other’s (controlled party) use of data that both know and that is not confidential under any traditional concept of confidentiality and that is not inaccurate in content. Not surprisingly, cases that have addressed questions of control of transactional data under traditional law typically find no privacy barriers against the use of the data other than where a traditionally confidential relationship was involved (e.g., doctor client).⁴ They do so because data control, whether or not it states a valid public policy, certainly states policies different and apart from traditional privacy law.

The issues in data control focus on allocating a right to control non-confidential information. Westin, for example, described “privacy” as involving the “claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”⁵ This description centers on control, rather than on protected secrecy, zones of privacy, or other interests associated with confidentiality. A later author described information privacy as “an individual’s claim to control the terms under which personal information -- information identifiable to the individual -- is acquired, disclosed, and used.”⁶

The shift is away from protecting against wrongful acquisition or unauthorized disclosure or use of private information of a sensitive nature and toward a broader claim of a right to control all information personally identifiable to the individual involved. The European Union Directive that contributes significantly to debate on this issue refers to “data protection,” essentially reflecting a property rights image in the form of the data owner’s right to have her information protected in the hands of the person to whom it was delivered.

The focus becomes “personal information” or “personally identifiable” information, rather than “private” information. The European Union Data Protection Directive, for example, defines “personal information” as any information relating to an identified or identifiable natural person “[who] can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”⁷

The comparison between this approach and traditional privacy law is vivid. A data control perspective limits one person’s right to use information that is personally identifiable to the other party. In contrast, cases applying traditional privacy law routinely hold that delivery of information to another party relinquishes privacy claims with respect to that information unless the relationship of the parties involves explicitly agreed or traditionally recognized indicia of confidentiality.⁸ Essentially, no reasonable expectation

⁵ Westin, Privacy and Freedom 7 (1967).
⁷ Data Protection Directive art. 2(b).
⁸ See Dwyer v. American Express, 273 Ill. App. 3d 742, 652 NE2d 1351 (1995). See also State v. Simmons, 955 SW2d 752 (Mo. 1997)(court held that defendant
of privacy exists. Each person is presumptively free to use that information in whatever way the person chooses subject, of course, to not creating actionable harm by its use.

**Language and Assumptions of Data Control**

United States law, in most respects, approached use of transactional data as primarily an issue solved by agreement of the parties. The agreement is made against a background that assumes that each party is ordinarily free to use information created or obtained in a transaction. Data control would alter that presumption, replacing it with an assumption that transactional information identifiable to an individual is restricted in use by the other party. The obvious question is “why”?

In understanding the answer to this, we need to begin by understanding further the language of data control, and the assumptions implicit in some of this language. The modern tendency of advocates of increased control rights has been to focus on the language and images of property rights and of government regulation. Both focuses tend to dictate outcomes that are independent of agreement by the affected parties. Since we are dealing with an environment that, by definition, involves voluntary exchanges between parties, this focus on mandates to the exclusion of contractual or interactive voluntary adjustments is telling. In part, this emphasis may reflect a desire on the part of activists to use privacy issues to justify increasingly intrusive regulation of aspects of commerce and social interaction.

Regardless of the rationale, however, a focus on property rights and regulation deflects attention from the interactive and voluntary character of the context in which data are created, transferred and maintained. If we look at that context, we see an environment of agreements, relationships, market choices and social interactions voluntarily undertaken. In that interactive context, it is neither awkward nor improper to protect and rely on the voluntary choices themselves, individually and collectively, to shape an appropriate allocation of data control interests. Law should intervene only when and if needed to correct results where the risks of harm are so significant that the need to control clearly outweighs the social and economic cost of that regulation.

**“Rights-talk” and Property Issues**

Let’s take a brief look at the language involved.

Property “rights-talk” is a major part of the privacy law debate from the perspective of control activists. This language emphasizes terms such as ownership, rights, infringement, waiver and the right to exclude. The assumption embedded in this approach is that one person owns (or should own) the data and that this person thus can enforce ownership rights against another party by precluding uses of the data by that other person. Those rights bind the other party unless the owner voluntarily waives or relinquishes those rights.

For advocates who use rights-talk in discussing data control themes, the data subject (person about whom the data relate) is the private individual and is also the person in whom rights should vest or in whom the activist assumes that rights have always vested. Those rights are seen as good and enforceable against the controlled party, which is most often assumed to be the corporation with whom the individual transacts, but more generally is any other party to the transaction.9

---

9 There is, of course, a circle here in cases where both parties are private individuals. Conceptually, rights could attach to both parties, setting up a form of double blocking
Rights-talk permeates “privacy” literature and law, although there are few publications that make a formal argument that privacy law creates property rights in personal data. This approach to the policy debate is used, one suspects, because rights-talk implies that the owner is in a position to waive or refuse to relinquish rights in its information and that any waiver is in effect a transfer from the owner to the other party. Once law identifies the owner of the rights, the argument is that law should prevent those rights from being infringed or taken away without the owner’s true consent. Thus, one policy underpinning for data control laws is claimed to be the need to protect and preserve the “rights” of individuals against corporate or other interference.

As applied to non-private transactional data, rights-talk has many flaws that prevent it from providing a useful model for analysis in most cases. The most basic weakness lies in the assumption about property rights ownership of transactional data. The assumption that the individual owns the data, of course, potentially answers the policy issue without more, but the assumption itself is not premised on a meaningful policy analysis. Indeed, transactional data are created or exchanged by parties to a transaction. If Party A and Party B enter into a transaction for the sale of a car for a stated price, which party owns the information about the transaction? The transactional data might be the following:

On July 1, at four in the evening in New York, Party A of 11 Post Street purchased Party B’s Mercedes for $38,000 cash. Party A received the car and the title certificate at that time.

This is transactional data of the purest type. But what is the basis of the claim that Party A, a private individual in New York, owns this data unless she waives ownership rights and why does Party B not have a similar claim, whether B is an individual or a company?

A contrasting premise of co-ownership, or at least, of a co-equal right to use data from a transaction reflects traditional U.S. law on this subject, although the concept has not been described ordinarily as an issue of ownership.

“Regulation-talk” and Government Control

“Regulation-talk” speaks in terms of rules, mandates, regulation, compliance, and agency oversight. The assumption, ultimately, is that markets and other voluntary interactions are failing or will fail to produce the results desired by the party advocating regulation and that, therefore, government intervention is required to reshape the interaction in appropriate ways. As with “rights-talk”, the themes of regulation-talk are a common, widely used aspect of the data control movement. Underlying data control policy, thus, is a judgment that markets do not and will not protect that which the control advocates believe should be protected.

A regulatory premise clearly has some narrow role in a market economy and a voluntary social context. But the data control activists typically describe data control needs in comprehensive terms, covering the entire economy, rather than merely those narrow aspects in which a definable market failure or extreme risk of harm exists. It cannot be the case that there is a market failure or high risk of injury in reference to all transactional data throughout the economy. The premise thus becomes less of a question of selective failure and more of a rejection of the idea of markets and voluntarily shaped interactions in general. This, indeed, may be an underlying premise of data property right. In practice, however, data control rules tend to cut through this problem by 1) excluding pure “consumer” interactions, and 2) defining individuals as not protected when they act as part of a business enterprise. See discussion at notes ---.
control law - individuals cannot control or shape their interactions in the marketplace with corporate entities and, therefore, regulation should be inserted.

As the breadth of regulatory scope is expanded, however, the policy increasingly implicates restrictions on the First Amendment speech activities of the controlled party. Data controls established by agreement or voluntary assumption of an obligation generally do not offend First Amendment values, but when the controls are regulatory, far greater limitations are imposed by the First Amendment. Data control as a regulatory issue thus faces obstacles in the form of constitutional restraints on government intrusion into personal conduct.

**“Contract-talk” and Agreed Allocations**

Transactional data is the product of voluntary interactions among two or more persons. In many cases, these interactions involve contractual or pre-contractual relationships.

“Contract-talk” themes emphasize terms such as agreement, exchanges, performance, expectations, and markets. The basic premise, ultimately, is that individual agreements or collective decisions made in a market yield the most efficient exchanges of value and sustain and support autonomy and individual choices in the economy.

From a contractual perspective, transactional data should be viewed simply as part of the exchange between the parties and the question should be to determine how the parties’ agreement handles the right to use or control that data. Transactional data can play several different roles in an exchange and that, ultimately, makes its relationship in respect to the parties complex. In some cases, it merely describes what occurred. In others, transaction data are part of the value exchanged, thereby defining at least in part the subject matter of the transaction. In still other instances, transactional data primarily serve to provide information about issues relevant to the other subject matter and its value to the contracting parties. This complex and variable relationship itself argues that caution should be exercised in altering it, because without information about specific contexts or narrowly defined general settings, rules appropriate for one interaction may be widely off the mark for others. That, of course, is another way of saying that individualized choices are better suited to dealing with the nuances of individual preferences and contexts under a contract law model.

Objections to a contract approach are typically grounded in an express or at least implicit rejection of the idea that markets work or that voluntary choices actually occur. The more narrowly focused of such objections might argue, for example, that in some situations no valid choice can be exercised because one party so totally controls the bargaining leverage as to over-ride choices by the other, or because the other lacks sophisticated understanding of the risks and opportunities among which it is or should be choosing.

**Selected statutes:**

### A. Organization for Economic Cooperation and Development (OECD)

**Guidelines proposed a set of eight principles:**

1. **Collection Limitation Principle.** Data collection should be with the knowledge or consent of the subject and by fair means.
2. **Data Quality Principle.** The data should be relevant to the purpose for which collection occurred and should be kept accurate, complete, and current.
3. **Purpose Specification Principle.** A purpose should be specified at or before collection.

4. **Use Limitation Principle.** No disclosure or use should occur for purposes other than the specified use without consent of the subject or authorization by law.

5. **Security Safeguards Principle.** There should be reasonable precautions to protect data against loss and unauthorized access.

6. **Openness Principle.** Policies, practices, and the existence of the data should generally be open rather than concealed.

7. **Individual Participation Principle.** A variety of rights should be given to the individual to verify the existence of data concerning him or her, to obtain the information, and to correct any data relating to him.

8. **Accountability Principle.** Persons who control the data are responsible for compliance with national law regarding the data protection rules.

**B. European Data Protection Rules**

The European Union Data Protection Directive spells out comprehensive standards for establishing a concept of fairness in data protection for individuals about whom personal data is being handled by a third party. The EU Directive, which states as a basic proposition that the joint goals of protecting personal privacy and avoiding restrictions on the free flow of personal data based on privacy concerns among member countries are essential to the evolution of the integrated market in Europe. The EU Directive applies to essentially all public and private data files, other than data compilation and processing relating to purely personal uses. The primary subject matter centers on processing “personal data,” a term that refers to information subject to being connected to an identifiable individual.

Under a data protection policy, a fundamental policy requires assurances concerning the quality and accuracy of the data collected and processed. The Data Protection Directive states this in a number of principles concerning data quality, construing the idea of quality in broad terms. Under these principles, the data must be:

- Processed fairly and lawfully
- Collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes
- Adequate, relevant, and not excessive in relation to the purposes for which they are collected or further processed
- Accurate and, where necessary, kept up-to-date
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed

---


12 EU Directive art. 2(a).

13 EU Directive art. 6.
A fundamental threshold protection in the EU Directive concerns the right of the individual, having been informed of the intentions of the data-processing entity regarding handling and collection of the data, to prevent that processing from occurring unless the subject “unambiguously consents” to that step or the processing fits into categories necessary for business operations. This structure balances between the most difficult and demanding data protection standard (a requirement of affirmative consent) and business operational needs which could be served by an implied consent standard based on information coupled with a failure to object on the part of the subject. The dispute between these two approaches was an important aspect of the early debate on the EU Directive.

According to Article 7, the situations not requiring unambiguous consent include the following:

1. Processing necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract
2. Processing to comply with a legal obligation to which the controller is subject
3. Processing necessary to protect the vital interest of the data subject
4. Processing necessary for the performance of a task carried out in the public interest
5. Processing necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection under Article 1(1)

For activities within the exemptions, the rights of the data subject to preclude data processing of personal data are framed in terms of a “right to object.” An overriding right to object is mandated at least with respect to processing concerning a legitimate interest of the controller of the data, but that right is to be based on “compelling legitimate grounds relating to his particular situation to the processing of data relating to him.” A less encumbered right to object arises when the anticipated use of the data involves direct marketing. The objection right in such cases is essentially absolute.

The obligations distinguish cases where the data is collected directly from the individual and cases where data is collected from other sources. In cases where the collection occurs directly from the data subject, the data controller must disclose the identity of the controller and the purposes of processing for which the data are intended. In addition, the disclosure must cover additional information necessary in light of the circumstances to guarantee fair processing for the data subject. These additional disclosures are to include materials such as the intended recipients or categories of recipients of the data, whether response to data-inducing questions is obligatory or voluntary, as well as the possible consequences of the failure to reply and the existence of rights to access and correct the data.

The disclosure obligations arising when the data is not obtained directly from the subject are similar, but the flexibility accorded to reduce the obligations on the data controller is more extensive. The disclosure must occur at the time the data is recorded or when the data are first “disclosed” to a third party. The disclosure must refer to the purpose of the processing, identity of the processor, and information such as the categories of information involved and the recipient or category of recipients for disclosure. These obligations do not apply, however, where the provision of the

14 EU Directive art. 7.
disclosure proves impossible to carry out or involves a disproportionate effort, or recording or disclosure is expressly required by law.

The EU Directive requires that data be held under secure and confidential conditions. Employees of the data controller cannot disclose the data except under instructions of the controller or by order of law. In addition, the controller must implement “appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorized alteration, disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.” Adequate measures are gauged by reference to the state of the art and the costs of implementation, but must ensure a level of security appropriate to the risks represented by the processing and the nature of the data. The EU Directive entails a regulatory approach and mandates the creation within each country of supervisory bodies to monitor the application of the law within the country.

C. California Security Breach Law

This statute deals with security issues. The statute, which applies similar provisions to governmental agencies and to businesses that conduct business in California, states that a business that owns unencrypted, personal information as defined in the statute must disclose any security breach of its computer system “to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” If someone else owns the data, such as when the business is processing data for another business, then the business suffering the security breach notifies the owner of the data (assuming that can be determined). The intention is to warn those whose data may have been compromised so that they can take appropriate steps, or to force governmental and private holders of information to encrypt it in order to avoid application of the statute.

The statute provides, in relevant part:

(a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

---

15 Cal. SB No. 1386, Ch. 915 (9/25/02). The statute, effective on July 1, 2003, adds Cal. Civ. Code §§ 1798.82 and 1798.29, relating to personal information.
16 See, e.g., Cal. Civ. Code § 1798.82(e): “For purposes of this section, “personal information” means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number; (2) Driver’s license number or California Identification Card number; (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.”
(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(f) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, “notice” may be provided by one of the following methods:

1. Written notice.
2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
3. Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:
   A. E-mail notice when the person or business has an e-mail address for the subject persons.
   B. Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.
   C. Notification to major statewide media.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.