Comparative Contractual Privacy Law: The U.S. and EU

By Paul Schwartz

I. Introduction
The law in the United States has long approved of and relied on individual authorization, explicit or implicit, as a legal basis for agreement. In the European Union, in contrast, a strong attempt has been made to limit the unbridled use of contract. The EU has built on this tradition in demonstrating profound skepticism towards contract in "data protection law," which is the European term for information privacy law. European law, whether at the European Union level or in the Member States, is deeply concerned about power imbalances between data processors and individuals. It resists reducing grounds for the legitimacy of data processing to notice-and-choice and places certain kinds of data use beyond contract. The General Data Protection Regulation, now under debate in Brussels, takes a similar hardline towards contract.

Yet, the U.S. offers a surprise in how it views contracting in the context of information privacy law. As concerns consumer contracts, it has created a kind of quasi-contractual regime, spearheaded by the FTC, in which, first, privacy and security promises must be made—and in writing. The second step is one in which the FTC not only holds these statements binding and polices deviations from their terms, but in some instances, goes further in limiting certain one-sided standardized terms and in requiring substantive requirements for data security. The result falls short of the strict EU rules around contracting for personal data. But the U.S. approach also deviates from contract law as practiced elsewhere in the U.S., where standardized terms tend to be accepted and upheld. This paper explores the differing views in the U.S. and EU towards the use of contract law as part of information privacy and data security law. It sketches notable divergences at the level of both legal principles and policy approaches.

II. Comparative Approaches to Contract
No man is an island, and generations of comparative law scholars have demonstrated that no legal system exists free from the influence of others. Contract law in the U.S. and Europe have long exercised an influence on each other. Friedrich Kessler stands as a prominent example of an influence from the German-tradition with his successful transplant of the concept of “contracts of adhesion.”\(^1\) Allan Farnsworth has also identified a reverse influence of common-law contracts on the rest of the world. The key exports from the American tradition are the ideas of leasing and factoring as well as “prolix drafting styles.”\(^2\)

---

\(^1\) Friedrich Kessler, Contracts of Adhesion, 43 Colum. L. Rev. 629 (1943).
\(^2\) E. Allan Farnsworth, Comparative Contract Law, 898, 904 in Oxford Handbook of Comparative Law (Mathias Reiman & Reinhard Zimmermann, eds. 2006).
Despite this shared aspects of the law of contracts in these legal systems, this paper is largely interested in differences. This Part sketches some of the most salient areas of divergence between U.S. and civil law systems regarding contract law. It then draws on this background to present two working theories of how these two systems are likely to structure contact law in the context of privacy.

A. The U.S.

The American legal system has long been friendly towards contractual ordering. In 1974, in a famous series of lectures, Grant Gilmore looked back on classic legal theorists and their doctrinal lines and wondered at “the narrow scope of social duty which they implicitly assumed.” Their world was one of the devil taking the hindmost, and the race being to the swift. In summing up classic contract law, Gilmore, with disapproval, saw a system that would “work ultimately to the benefit of the rich and powerful, who are in a position to look after themselves and to act, so to say, as their own self-insurers.” With apparent relief, Gilmore welcomed a development that he perceived underway, namely the “transition from nineteenth century individualism to the welfare state and beyond.”

As it turned out, however, the victory of “the welfare state and beyond” proved far less complete than Gilmore anticipated in the 1970’s. From a contemporary perspective, and to revise Gilmore’s celebrated central metaphor, contract did not die. Without diminishing the achievement of these lectures, we can identify the more accurate crystal ball as belonging to Robert Braucher, then Professor of Law at Harvard Law School, and soon to be a Justice on the Massachusetts Supreme Court. Conceding in 1969 that “freedom of contract” was “not the ringing phrase it once was,” Braucher assessed the then current draft of the Second Restatement of Contracts and concluded, “Freedom of contract, refined and redefined in response to social change, has power as it always had.”

Today, U.S. courts routinely upheld contracts that Gilmore would likely view as a dubious bolstering of the position of the “rich and powerful.” The general rule is that of enforcement of non-bargained or otherwise one-sided agreements expressed in standardized contracts, Terms of Service, or a variety of click-through screens. These agreements, in turn, constitute most of the actual contracts with which Americans contend. As Lewis Kornhauser already perceived in 1976, a large proportion of contractual agreements, perhaps as many as ninety-nine percent of them, “do not conform to the pattern of interaction, dickering and other bargaining required by contract law.”

We live in a world of enforced boilerplate, and, for many concerned scholars, one of vanishing individual rights. Margaret Radin has described the phenomenon as one in which legislatively granted interests are canceled by the effect of standard

---

4 Id.
5 Id.
terms. She observes, “Mass-market systems of form contracts that restructure the
rights of users of products and services operate to undermine or cancel the rights of
users granted by legislatures.” As an example, unread Terms of Service are held to
trump legislation concerned fair use in copyright and to restrict creative use of
information. Nonetheless, the U.S. approach to contracts is one largely favorable to
letting parties reach agreement on their own terms, even if the classic ideas of
bargaining and “meeting of the minds” are acknowledged today to be more fiction
than reality.

B. The EU

As in the U.S., the continental tradition values freedom of contract. During the
last half-century, however, a decisive movement has been underway to build
protections against many types of unfairness into the framework of contract law.
Within the continental traditional, German law has distinguished itself through its long
attention to the fairness of standard terms. This focus, beginning first in the courts,
shifted to the legislature with the enactment of the 1977 Act for the Control of the
General Conditions of Business (Allgemeine Geschäftsbedingungen Gesetz, AGBG).
In comparison to the Uniform Commercial Code, the AGBG distinguishes itself by its
rich detailing of unfair terms and the ongoing legislative amendment of it. First
enacted outside the German Civil Code, the BGB, the AGBG has now been
incorporated within it. 9

Another point of comparison is the effect of constitutional law on contract law.
In the U.S., the Supreme Court’s Lochner decision represented an extreme in the use
of constitutional law and contract law principles to prevent social regulation. 10 For the
Lochner Court, a state law limiting the working hours of bakers was an
unconstitutional infringement of their freedom of contract. The Supreme Court
ultimately rejected this idea in West Coast Hotel v. Parrish: the State is free to
regulate economic activities, and the Due Process Clause is not to be used to strike
down laws in the name of freedom of contract. 11 Even with the end of Lochnerism,
however, the U.S. Constitution remains one of negative rights. It does not oblige
the State to take positive steps to create conditions that will allow the existence of
fundamental rights. Rather, it provides rights that allow the individual to stop certain
kinds of state action that interfere with fundamental rights.

In the E.U., in contrast, more modern constitutions call for an active role of the
State in establishing and preserving constitutional conditions within society. For
example, the German constitution document, the Basic Law (Grundgesetz), both limits
the state and sets positive goals for it to achieve. Reaching these goals require State

---

8 Margaret Jane Radin, Boilerplate 16 (2013).
9 Section 305ff. Bürgerliches Gesetzbuch [BGB] [Civil Code] BGBI. I S. 42, ber. S. 2909 and
BGBI. 2003 I S. 738; Graf v. Westphalen, AGB-Recht im Jahr 2014 [Control of the General
10 198 U.S. 45 (1905).
activities in the spheres of "private" and "public" law alike. The German Federal Constitution Court has taken an active role, in turn, in interpreting the Basic Law and establishing the reach of constitutional rights into relations between citizens, including into their contracts. For our purposes, we can leave to the side the interesting and complex question, widely explored in caselaw and scholarship, about how German fundamental rights are best to be integrated into relations between private parties. Issues here include the debate about the direct or indirect impact of fundamental rights. More to the point of this paper, in legal systems throughout Europe, including Germany, the Netherlands, and Italy, the judiciary has drawn on constitutional rights to evaluate the bargaining positions of parties and to protect weaker parties.

Finally, there is the influence of EU law on contract law. Indeed, this area offers one of the leading examples of the phenomenon of the Europeanization of private law. The EU has enacted a series of consumer protection directives with a considerable impact on contracts. These include the Doorstep Selling Directive (1985), the Consumer Credit Directive (1987), the Package Travel Directive (1990), the Unfair Terms in Consumer Contracts Directive (1993), the Timeshare Directive (1994), and the Distance Selling Directive (1997). These Directives, which are then transposed into national law in EU Member States, have provided European consumers with greater protection than American consumers typically are offered from boilerplate. For example, the Unfair Contract Terms Directive's basic rule is that a contract term that is not individually negotiated is "unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer." This Directive also contains an Appendix with a long, non-exclusive list of terms that may be deemed unfair. As Jane Winn and Martin Weber summarize the impact of EU Directives in this area, "The development of contract law on unfair terms in Europe over the last 25 years is an important change in EU contract law that has no direct counterpart in U.S. contract law." Specifically, Winn and Weber conclude that the Unfair Contract Terms Directive "establishes a much lower threshold for intervention

---

by courts and regulators than unconscionability under U.S. contract law or federal and state regulation of unfair and deceptive trade practices."

C. Two Working Theories

Before turning to information privacy regulation, we might hypothesize how law in the U.S. and EU are likely to treat contracts in this setting based on our knowledge of their underlying approach to contracts. One would expect the U.S. to be contract-friendly and ready to enforce a wide range of boilerplate about personal information use. To be sure, some American scholars have decried enforcement of unread standardized terms. Other scholars, those of the law-and-economic persuasion, have generally encouraged us to relax about this situation and identified certain benefits of real-world contractual “imperfections.” We can learn to love “rational ignorance” when faced with the daily onslaught of a variety of standardized term contracts. From the law’s perspective, in a universe of asymmetrical information and limited bandwidth on the part of consumers, we might wisely focus on whether a standardized contract rewards productive investment in information. From that perspective, many contracts that do not result from a bargain should be upheld. Our working theory for U.S. information privacy law would therefore be that the data gatherers and processors would be viewed, in many circumstances, as engaged in productive activities, that the law would sympathetically view their attempts to set the terms of information exchanges, and privacy boilerplate would be upheld, read or unread, understood or not.

For the EU, we would expect a strenuous effort to protect consumers from information privacy risks that arise in contractual settings. Here, we can also expect the influence of constitutionalization to be felt. Indeed, European constitutional law does more than stop unfair contracts. Its attention to the privacy as a human right is enshrined in cornerstone documents of European integration. These include the European Convention of Human Rights (1950), whose Article 8 grants everyone a "right to respect for his private and family life, his home and his correspondence." More recently, an explicit "right to protection of personal data" was declared in Article 8 of the European Charter of Human Rights, which became legally binding with the Lisbon Treaty entering into force in 2009. Our working theory for European information privacy law would therefore be that it would be skeptical of contracts and attempt to cabin its use.

III. The US Approach to Information Privacy

Unlike EU law, U.S. law does not place special requirements on international data transfers involving personal data. Like EU law, however, U.S. law has confronted legal issues regarding the use of privacy contracts in consumer and commercial settings. Regarding business-to-consumer agreements (B2C), the caselaw is thin, but in the handful of cases on the topic, U.S. courts have not held privacy policies to be contracts. The development of this area has not by common law courts, but at the federal agency-level and through legislation and regulation. In particular, the FTC has developed a quasi-contractual law of privacy. Here, we see a surprising correction to our first working theory.

---

Regarding commercial contracts, that is, business-to-business agreements (B2B), an important development has been the law’s growing requirement for written contracts in which initial data collectors require compliance with privacy and security obligations from their vendors, business associates, and other parties with whom they share personal information. Enforcement actions of the FTC have similarly paid attention to forcing compliance down the chain of entities that come into contact with personal information. This development is not inconsistent with the working theory's prediction of a contract-friendly privacy universe. It shows reliance on contract, but one in which the terms of the contract are largely dictated by an agency, statute, or regulation. Hence, here too, we are far from the standard universe of U.S. contract law.

A. B2B: The FTC and Quasi-Contractualism

Regarding B2C agreements, there are only a handful of cases that explore the role of contract law in information privacy law. These cases show courts to be contract-skeptics when judging information privacy litigation. As an initial example, the district court in In Re Northwest Airlines Privacy Litigation declared that the privacy policy on the airline’s website did not constitute a contract.²⁰¹ Plaintiffs had alleged that Northwest had violated its promise that information it collected would be used only for limited purposes. The airline had, in fact, shared extensive consumer data with a federal agency to assist its study of airline security.²⁰² For the Northwest court, these promises were only “general statements of policy.”²¹ Other courts have struggled to find damages when companies fail to uphold their commitments regarding personal data use. Thus, in another case involving airline passengers’ personal data, the district court in In re Jet Blue Airways Corp. Privacy Litigation declared, “There is … no support for the proposition that an individual passenger’s personal information has or had any compensable value in the economy at large.”²²

Other cases demonstrate additional judicial doubts as to the merits of contract law in the context of information privacy. Rather than any notable judicial leadership, the FTC, with an assist from federal and state legislation and regulations, has played the critical role in creation of a quasi-contractual law of information privacy. This body of law, made up of enforcement actions and settlement orders, sounds in contract, but does not focus on offer and acceptance, or bargaining between private parties. The central paradigm is also far from any concern with a “voluntary assumption of obligation.”²³ Rather, federal agencies and the legislature first require written language to be in place about data processing and data security. This area of law then uses this written language as a starting point first for in searching for deception and then in developing normative requirements for required and forbidden practices.

---

²⁰² Id. at *5.
²¹ Id. at *6 (quoting Martins v. Minn. Mining & Mfg. Co., 616 N.W.2d 732, 741 (Minn. 2000)).
1. Binding Statements of Practice. One of the most striking aspects of this quasi-contractual process is the wide range of institutions involved in requiring privacy and security practices be expressed in writing. A patchwork of such obligations is now found in federal law, FTC actions, and state law. The federal authorities include the Gramm-Leach-Bliley Act (1999), which regulates financial institutions; the Cable Act (1994), which regulates cable companies; the Children’s Online Privacy Protection Act (1998), which regulates websites that collect information about children under the age of 13 years old; and the HIPAA Regulations (2002), which require “covered entities,” that is, hospitals, other health care institutions, and physicians who file for insurance payments electronically.

These federal authorities, while far-reaching, still fall short of covering the entire U.S. economy. Remaining gaps regarding a requirement for organizations to declare privacy and security policies in writing have largely been closed, however, by the FTC and state law. Pursuant to its Section 5 authority, the FTC has identified a requirement that companies under its jurisdiction disclose the extent of their personal data gathering and information processing. A company that fails to do so would likely be engaged in an unfair or deceptive trade practice.

A further contribution to this legal web imposing a requirement of notice occurred at the state level. In a decisive demonstration of the value of privacy federalism, the Golden State in 2003 enacted the California Online Privacy Protection Act (CalOPPA). This statute was the first law in the nation to require online companies to post a privacy policy in an accessible part of its website. Due to the size of the California economy, the largest in the United States and ranked seventh in the world, it is hardly feasible for companies to ignore CalOPPA. The impact of these federal and state requirements is clear: organizations that collect information from consumers should state their privacy policies in writing and make these statements publicly available.

2. Enforcement of Privacy and Security Statements, Development of Substantive Requirements. As we have seen, courts generally do not think that written expressions of data handling practices represent part of a contract. But the FTC has taken a different approach to these documents, and one that has been decisive in creating a quasi-contractual information privacy law. The FTC has enforced promises made and even created substantive requirements for data handlers. As Daniel Solove and Woodrow Hartzog have argued, “FTC privacy jurisprudence is the broadest and most influential regulating force on information privacy in the United States.”

25 Cal. Bus. & Prof. Code § 22575 (West 2014). This statute has been subsequently amended, most recently in 2014, to specify additional kinds of information to be included. The 2014 amendment requires companies to state how their websites respond to Do Not Track requests.
26 Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Colum. L. Rev. 583, 587, 589 (2014) (noting also that the resulting body of FTC enforcement actions, nearly two hundred settlement orders, and staff opinions create a "rich jurisprudence that is effectively the law of the land for businesses that deal in personal information.").
To extend the Solove-Hartzog analysis, I would say that the FTC’s behavior in this setting is similar both to a common law court and a legislative body. Like a common law court, it has policed against broken promises and deceptive language, albeit through settlement actions rather than formal litigation. Like a legislative body, however, it has removed certain requirements from bilateral negotiations and shaped the terms on which agreement may occur. The end result is far from full-blown EU data protection law, but it also marks a decisive deviation with the typical US approach to standardized contractual terms.

Over the last decade, in particular, there has been a decisive evolution by the FTC beyond its previous policing of broken promises alone and its initial reliance on a barebones jurisprudence of “notice-and-choice.” By the late 1990’s, it seemed that a kind of digital caricature of 19th Century “freedom of contract” was established in information privacy law. The idea was a privacy statements of an online company provided “notice” and the consumer’s visiting of a website constituted “choice” to data collection and future data use. The FTC policed largely against broken promises, which occur when a company promises one thing in its privacy or security statement and then engages in different behavior. For example, a company might promise not to share customer information and then share the information anyway. The FTC also objected to companies making retroactive changes without informing the affected consumer and obtaining her consent.

The era of exclusive "notice-and-choice" enforcement proved only an initial stage in the FTC’s path toward developing substantive requirements for fair conditions of data processing and security. Over the last decade, the FTC has looked more broadly to the terms of privacy notices to punish a variety of deceptive practices, actions that it finds to be unfair, and, more generally, to block corporate overreaching. Thus, it has alleged unfairness in a practice, even when disclosed in a company’s boilerplate, that seemed unexpected due to the intensity of the invasion of privacy.27 In this last instance, which occurred in the Sears enforcement action, we see a classic judicial move of policing contracts against unexpected terms, even when they are found in boilerplate available to the consumer.

Beyond this role, the FTC has identified substantive requirements for companies to follow to safeguard data security. As an initial example, the FTC considers a failure to properly train employees regarding security as an unfair practice. The FTC has also settled enforcement actions against companies that fail to follow industry standard practices, regardless of the promises that the organizations made. As a further example, and one concerning privacy, the FTC has engaged in behavior that Solove-Hartzog aptly term "qualitative."28 These include establishing baseline standards for behavior based on a combination of industry norms and the FTC’s own assessment of reasonable expectations about data collection practices, an evaluation which inevitably involves the agency in making normative judgments.

27 In 2009, Sears ran afoul of the agency by burying important information in a long user license agreement regarding the extent of its tracking. Sears Holdings Mgmt. Co., F.T.C. No. 082-3099 (2009), 2009 WL 2979770. But it had not included clear information about this undoubtedly unexpected practice: downloading the application in question would lead to the tracking of nearly all Internet activity on consumers’ computers.
28 Solove & Hartzog, supra note 26, at 658.
B. B2B

In the context of B2B-relations involving personal data, the law increasingly turns to contract. More specifically, it increasingly requires contracts and, indeed, specifies substantive content for these documents. If the main developments regarding contracting about personal information use in the B2C-context prove FTC-centric, a variety of statutes, regulations and federal agencies have demanded use of contracts for commercial entities who share information. The law has used contracts to spread requirements originally placed directly on sectorally-regulated organization to the many vendors, business associates, and third parties with whom data are shared.

The HIPAA Regulations provide a good illustration of this process. HIPAA itself is legislation focused around the portability of insurance. Due to congressional inability to agree on privacy standards, the Department of Health and Human Services (HHS) promulgated regulations, under a grant of congressional authority, for privacy (2002) and then for security (2003). In 2009, Congress enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act. This statute sought to facilitate the move to electronic health records in the U.S.; it also strengthened the various HIPAA regulations and, in particular, created an obligation for greater vendor management by covered entities. In turn, the HHS implemented the mandates of the HITECH Act as part of its Omnibus Regulation (2013).

This iterative collaboration between Congress and HHS has led to strong requirements for all HIPAA “covered entities” to contract with their "business associates" (BA’s). The latter are entities that provide functions or activities that involve the use of protection health information on behalf of a covered entity. HHS Regulations provide significant detail as to the content of the required contracts. These agreements must describe the permitted use of protected health information by the BA, place strict limits on future BA use of data, and require the BA to use appropriate safeguards for data security. A BA must enter into the same kind of contracts, moreover, with any subcontractor that it uses. Finally, the covered entity must respond to any “pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract” by taking “reasonable steps to cure the breach or end the violation.” If unable to cure the breach or end the violation, the covered entity is either to terminate the contract, if feasible, or report the problem to HHS.

This trend of pushing enforcement down the data chain is found elsewhere in privacy law. For example, the Dodd-Frank Act gives authority to the Consumer Financial Protection Bureau (CFPB) to examine supervised banks and nonbanks for

---

compliance with federal consumer financial law. Mortgage companies are among the entities that fall under this provision. In a 2012 Bulletin, the CFPB indicated that the entities that it regulates must enter into contracts with their service providers. It expects the regulated entities “to oversee their business relationships with service providers in a manner that ensures compliance with Federal consumer financial law.” Among other mandated behavior, these contracts are to indicate “appropriate and enforceable consequences for violations” of federal consumer financial law.

IV. The European Approach to Data Protection

Our point of comparison for European law will be two important EU instruments: the European Data Protection Directive and the draft General Data Protection Directive, which is destined to replace it. As early sections of this paper have shown, the general European approach to contract has long been a more skeptical one than in the U.S. Our working theory for EU law is to expect a strenuous effort to protect consumers from information privacy risks that arise in contractual settings.


Enacted in 1995, the EU Data Protection Directive is a “harmonizing” instrument. It is not directly binding on Member States, but requires enactment of legislation that follows its commands. In this regard, it follows in the path of the many directives regarding consumer protection mentioned earlier in this paper. The Data Protection Directive permits use of contracts in two contexts. First, consent can provide a legal basis for a "controller," the person or organization that makes decisions about personal data use, to process such information. The Directive permits a party to collect and use personal information if it obtains valid consent from the affected individual, or "data subject." Such agreements generally concern B2C transactions. Second, a controller can use a contract as a legal basis for an international data transfer to a party in a non-EU country that does not provide sufficient EU-style privacy protections. These kinds of contracts are between two or more sets of enterprises and can be considered B2B agreements. In a nutshell, the EU Directive contains a narrow definition of consent, which strongly limits contracts between entities in the B2C category. In the B2B category, it has accepted use of contracts in establishing international data transfers. This latter issue is particularly important in the global economy.

39 Id.
40 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
41 Directive 95/46/EC, Art. 7 (a).
42 Directive 95/46/EC, Art. 26 no. 2.
1. B2C

Regarding consumer authorization of data processing, the Directive does not permit data processing without a legal basis. Here is a notable difference with the U.S., where the starting point is that personal data may be processed freely unless some legal justification limits this behavior. American lawyers looking at the Directive will initially be heartened by the presence of a contractual basis for data processing. This joy will largely end, however, once these lawyers learn how the Directive limits the use of consent as a justification for data processing. First, the Directive contains a strict definition of consent in its Article 2(h). Second, unlike U.S. law, in the EU, consent does not trump other legal requirements for data processing. In other words, even if there is consent, other conditions must be met before data processing is permissible.

As noted, the Directive's definition of consent is strict. It is also far from concisely worded. Pursuant to Article 2(h), consent is "any freely given and specific and informed indication of … wishes by which the data subject signifies his agreement to personal data relating to him being processed." As this term indicates, current EU law creates numerous hurdles before individual consent can be considered valid. For an official explication of this definition, one can turn to the Article 29 Working Party, an influential committee of EU data protection commissioners. The Working Party has developed a four-step test for gauging the validity of consent to data processing; all of these steps must be fulfilled for consent to be legally valid. These requirements are that (1) consent must be a clear and unambiguous indication of wishes; (2) consent must be freely given; (3) consent must be specific; and (4) consent must be informed.\(^{43}\)

The requirement that consent be "freely given," the second element, alone removes this justification for data processing \emph{a priori} from a number of situations. The Working Party has warned that "freely given" requires "no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent."\(^{44}\) As a result, the Working Party would refuse reliance on the consent justification for data processing when an individual lacks a genuine ability to withhold agreement. This group seeks to remove use of consent, for this reason, from agreements involving employment or health care treatment. Similarly, the German federal data protection law, the \emph{Bundesdatenschutzgesetz}, has long been highly skeptical of use of "consent" mechanisms in these two contexts.

This skepticism regarding the use of consent for employment or health care decisions has been more than matched by similar doubts about consent in online contexts. Both the Working Party and the Commission of the EU have expressed concern about the validity of consent on the Internet. For example, the Working Party cautions against the use of pre-ticked boxes on Internet forms to indicate consent. For the Commission, the executive branch of the European Union, it questions whether a user's consent to behavioral advertising can be delivered through browser settings.\(^{45}\) Even when valid consent has been given under Article 2, other elements of the

\(^{44}\) Id. at 12.
\(^{45}\) Id. at 3.
Directive limit its reach. For example, the Directive requires special consent, or in its terms "explicit" consent, for certain selective categories of information. In its Article 8, the Directive prohibits the processing of personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." While the Directive does not define "explicit consent," the consensus is that an opt-out solution does not meet this standard.

Beyond this requirement of explicit consent for the "special" categories, the second notable limit on the scope of general consent is that an individual authorization does not trump the Directive's other requirements for making data processing legally permissible. For example, consider Article 6's principle of "data quality." This term refers to a daunting list of substantive requirements, namely "fairness, purpose limitation, proportionality, accuracy, and data storage limitations." Even when adequate consent is in place, the concept of "data quality" sets further requirements on data use.

In sum, the Directive reflects a restrictive view of the bounds of a consent justification. In his treatise on EU data protection law, Christopher Kuner advises organizations to seek other paths under the Directive to justify their processing of personal data. He recommends that companies "reduce their reliance on consent as a legal basis for data processing to situations where it is absolutely necessary." (68)

Ironically, the Directive's strict approach to consent sometimes obliges a more frequent seeking expression of consent. In particular, and to return to Article 6, its concept of "purpose limitation" restricts the reach of any single consent. Article 6(1) states that personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." As a result of this provision, an authorization cannot be too broad and future use of data for any new purpose requires additional and new consent from the affected individual. For those skeptical of the worth of disclosure mechanisms and individual authorizations, the irony of the EU approach is that its restrictions on consent can lead to more disclosures and more authorizations and perhaps (further) reduce the comprehension of processing practices by the affected party.

2. B2B

In the EU, contracts provide an essential legal path for businesses to transfer personal data to enterprises in non-EU nations. Understanding this legal mechanism first requires some basics about international data transfers involving personal

---

46 It also provides a series of limited exception to this general ban on processing of these "special categories of data," including where the "data subject has given his "explicit consent" and Member State legislation has not ruled out use of consent in the specific situation.
49 As an example, the Working Party points that agreement to use of one's personal information to participate in online activities is not tantamount to consent for use of these data for other purposes, such as the delivery of marketing information. (23)
information of EU citizens. The EU permits the personal data of EU citizens to be sent outside of the EU only when "adequate" data protection is provided.\textsuperscript{50} On this side of the Atlantic, the policy challenge is that EU does not consider the U.S. to achieve this level. The implications of this view are significant. As Lothar Determann has observed, we live in a world of international data transmissions. He writes: "Few companies can satisfy themselves that they do not receive, use, host, or send personal data across jurisdictional bodies."\textsuperscript{51}

Fortunately, the EU has developed a number of solutions for countries, like the U.S., that it does not consider to meet its privacy standards. Until October 6, 2015, the key instruments for data transfers were the Safe Harbor agreement, Binding Corporate Rules, and contractual agreements. On October 6, however, the European Court of Justice (ECJ) invalidated the fifteen-year-old Safe Harbor agreement, which was a US-EU treaty. Under it, organizations in the U.S. had a much favored path for meeting the adequacy requirement. Companies first would publicly certify their agreement to certain principles for privacy and then would follow these requirements in use of personal information. Due to the Snowden revelations, the ECJ declared the Safe Harbor invalid on multiple grounds, including its lack of restrictions on the access of U.S. public authorities to personal data covered by the agreement, the lack of adequate means of redress for the persons affected, and the Safe Harbor’s limitations on the powers of EU national supervisory authorities.\textsuperscript{52} The invalidating of the Safe Harbor has made contractual agreements between organizations in the EU and US more important than ever before for international data transfers.

The EU has approved two sets of model contracts and also permits "ad hoc" contracts between enterprises.\textsuperscript{53} At the same time, it has created a set of procedural and other roadblocks to the use of such contracts in the B2B setting. Thus, the picture in the EU is one of skepticism towards contractual mechanisms in both the B2B and B2C context and at a time when these tools are more important than ever before in enabling international data flows involving personal data.

Scholars who praise standardized forms in contracting view them as allowing parties to concentrate on other aspects of dealmaking, such as price. By approving the model contracts, the EU has taken a step to lower the legal transaction costs of businesses that seek to transfer personal data outside of the EU. As a means towards this end, however, the model contracts are incomplete. The difficulty is that these

\textsuperscript{50} Art. 25, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
\textsuperscript{51} Lothar Determann, Determann’s Field Guide to Data Privacy Law 24 (2d Ed. 2015).
\textsuperscript{52} Schrems v. Digital Rights Ireland Ltd., Case C362/14 (2015).
“off-the-rack” documents leave considerable hurdles in place for data exporters and importers, which make the model contracts less than appealing.

The first set of contractual clauses contains an unappetizing requirement of joint and several liability for the two contracting parties. It also contains certain provisions that point to higher requirements than even that of the Directive itself. As for the second set of clauses, these were developed under the sponsorship of the International Chamber of Commerce and received EU approval in 2004. While privacy experts view the second document as more helpful than the first set of model clauses, it does not greatly streamline the process of transferring personal data to "non-adequate" countries. One issue is that the second set of contractual clauses come with a private right of action for the data subject. In one fell swoop, this contractual solution increases potential liability for data importers beyond that under Safe Harbor and Binding Corporate Rules, which have no such requirement.

For both sets of model contracts, a further issue is that Member State data protection commissioners can set additional requirements on companies that use these contracts. In his treatise, Kuner provides an appendix that details some of these additional legal requirements within a subset of the twenty-seven Member States of the EU.\(^\text{54}\) The bottom line: the model contracts have not led to standardized conditions for data exports. Information transfers that involve data flows from different Member States cannot be handled with a single legal approach.

As for customized or "ad hoc" contracts, the parties that use them bear greater transaction costs than under the model contracts because they must pay their lawyers for drafting and negotiation of contractual terms. As a further cost, many Member States require approval of each contract by the national data protection commission or commissioner. As Kuner warns, the result is "a time-consuming and expensive process, especially in the case of a complex series of transfers in which dozens or even hundreds of authorizations must be obtained."\(^\text{55}\)

**B. The General Data Protection Regulation**

With the goal of creating greater uniformity in data protection law in Europe, the EU is now replacing its Data Protection Directive with the General Data Protection Regulation (GDPR). At a basic level, uniformity generally follows from the choice of a Regulation rather than a Directive. Unlike a Directive, a Regulation does not require harmonizing legislation to take effect, but creates directly enforceable standards. Here, we see the EU advancing beyond the various consumer directives and its own Data Protection Directive. Under the GDPR, the approach to contractual terms is similar to that of the Directive. The story here is one of continuity.

**1. B2C**

Regarding B2C contracts, while the GDPR uses roughly the same definition of “consent” as the Directive, it heightens existing consent requirements. In consequence, and as one international law firm flatly states in its evaluation of the

\(^{54}\) Kuner, supra note 48, at 225.

\(^{55}\) Id. at 201.
Regulation: "[c]onsent becomes harder to obtain." In any processing based on consent, GDPR requires "the burden of proof" of a valid authorization to be on "the data controller." The “data controller” is the party who determines the purposes and means of the processing of personal data. The data controller must be able to demonstrate that affected individuals have agreed to the processing of their personal data for specified purposes. As existing German data protection law interprets these elements, for example, consent requires agreeing knowingly and deliberately to the specific purpose of processing the data.

Other heightened requirements for consent in the GDPR concern the conditions for written authorization and for allowing parties to withdraw consent at any time. Perhaps most importantly, and as a step beyond even placing the burden of proof on the data controller, the GDPR forbids the use of consent when "there is a significant imbalance between the position of the data subject and the controller." This approach builds on and heightens the Directive’s requirement that consent be "freely given."

The GDPR also contains the requirements for "data quality" found in the Directive. Like the Directive, it has a strong requirement of "purpose limitation." Information must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." Moreover, personal data must be "adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed."

2. B2B

As for B2B contracts, and, specifically, as regards international data transfers, the Proposed GDPR leaves much of the current system in place. For example, like the Directive, the GDPR permits ad hoc contracts. The text of the GDPR proposed by the Commission also permits the model clauses to continue as a valid transfer mechanism. Most significantly, however, the GDPR does not require any specific

---


57 COM (2012) 11: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Art. 7 no. 1. Note as well that the Council prefers a requirement that the controller be able to demonstrate "unambiguous consent."


59 COM (2012) 11: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Art. 7 no. 4.

60 Id at Art. 5 (c) .

61 In contrast, the Parliament would permit the model contractual clauses to continue in force only for five years after the Regulation is enacted. This sunsetting would restart the negotiations in Brussels concerning appropriate model clauses.
authorization from data protection authorities, renamed Supervisory Authorities, for cross-border transfers pursuant to the model clauses. Here, we see a productive step that would reduce transaction costs through contracting for international data transfers. More recent development within the EU have cast significant doubts, however, on the future of this “one stop shop.”

VI. Contracting and Privacy: Today and Tomorrow

The late philosopher and Yankee great Yogi Berra warned, “It is hard to make predictions, especially about the future.” Nonetheless, I wish to conclude with some observations about the future path of contract law in the context of information privacy and data security in the U.S. and EU.

A. Revisiting the Working Theories

We can begin by restating our two working theories about the use of contract law in the context of information privacy. Regarding the U.S., based on existing contract law jurisprudence, one might expect strong, and perhaps even unthinking enforcement of privacy boilerplate. In the EU, in contrast, we might expect a strenuous effort to protect consumers from unfair contracts through the law’s defining of those elements of contracts that are permissible and impermissible.

In the U.S., the FTC's development of a quasi-contractual law of information privacy provides a surprising correction of this paper’s first working theory. To be sure, there is no end of privacy notices that are tilted toward the data collectors and other entities engaged in the lucrative practice of “surveillance capitalism.” Yet, the FTC has developed standards that limit boundless boilerplate on grounds of unfairness and deception. The result falls short of the strict EU rules around contracting for personal data. But this approach also deviates from contract law as practiced elsewhere in the U.S.

The development by the FTC of its privacy standards has been controversial. For some practicing attorneys, the FTC has failed to follow established contract law principles regarding standardized forms of agreement. As Alan Raul and his co-authors argue, “mainstream principles of contract law” require upholding boilerplate agreements, such as that between Sears and its users regarding spyware. Recall that information about this extensive tracking by Sears was present in the agreement with the user, albeit buried deeply in Terms of Service. Raul and his co-authors state: “The provisions in Sear’s agreement were not obviously oppressive, especially in comparison to terms in standardized contracts that have been upheld, such as choice-of-forum [clauses].”

Based on a quasi-contractual approach, the FTC has used its Section 5 authority first to require privacy statements and then to police them and shape and reject terms in them. Rakoff has noted that "specialized administrative agencies … can become experts about matters in their particular domains in a way the general-

64 Id.
The FTC has developed great expertise in this area; even more so, it has developed and enforced standards based, at least in part, on its own sense of normatively-required and normatively-forbidden practices. Once organizations make statements in their privacy and security notices, the FTC enforces, polices, and parses these statements based not on contract law principles but on its evolving development of its organic act’s bedrock concepts of “unfairness” and “deception.”

These developments are interesting on a number of grounds. First, market forces have not disciplined the drafters of standard forms for privacy. Certainly, we do not have a small number of readers deterring overreaching by data collectors. Indeed, the empirical evidence points to almost no one reading privacy statements. The research findings are tracked by a truism in privacy law circles: “No one has ever read a privacy statement who wasn’t paid to do so.” Kornhauser identified a historic pattern in which the state removes the substance of some contracts from the exclusive power of the parties involved in the agreements. He writes, “When a state wishes to regulate the substantive contents of agreements, it looked to a substantive area of law: the law merchant, insurance law, labor law.”66 Regarding privacy and security, the FTC has acted and bolstered sectoral legislation by taking certain kinds of behavior out of the realm of bilateral agreement.

Second, there has been an unanticipated benefit of privacy notices, and one absent from usual theoretical analysis of standardized terms. There has been a chorus of voices pointing out that these terms are barely read by the public. But the process and effort of drafting these legally-required notices have created a valuable focal point within organizations. Already in 2002, Peter Swire, the top privacy official in the Clinton administration and a leading privacy scholar, identified this aspect of the privacy notices that the GLB Act requires. He wrote, “a principal effect of the notices has been to require financial institutions to inspect their own practices.”67 Once the inspection had been carried out, the regulated financial institutions took action. As Swire observed, “Related to this process of self-examination, many financial companies put in place new institutional structures for managing privacy and security.”68

As more statutes and the FTC required such privacy notices, organizations reached a critical mass of privacy and security related work and created institutional structures, such as Chief Privacy Officers (CPO's). Outside of the data processing organization, this privacy work has created a boom for privacy lawyers within Big and not-so-Big Law. Lawyers read and counsel their clients based on the resulting rich “caselaw” of FTC settlements as well as international developments and federal and state lawmaking. The market has also responded with a boom in privacy and security consulting services, including in external CPO's who work on an hourly basis.

As for the EU, as predicted in this paper’s second working theory, it cabins contract law strongly based on regulators’ sense of practices that are and are not

---

66 Kornhauser, supra note 7, at 1153.
68 Id.
acceptable. As a consequence, the two leading EU data protection instruments, the Directive and GDPR, limit the use of contract law in the name of protecting the "data subject." Here is how the Working Party 29, 2011 summed up the EU-wide skepticism about unbridled contractualism: "The more difficult it becomes for an average citizen to oversee and understand all the elements of the data processing, the larger the efforts should become for the data controller to demonstrate that consent was obtained based on specific, understandable information."^69

Contract law in EU privacy law fits comfortably within a tradition in EU law of skepticism towards leaving agreements only to the immediate parties involved. The societal consequences of contracts are too important for these agreements to be left to the immediate parties. To return, for example to the Directive on Unfair Contracts, its extensive and broad list of unfair terms far exceeds the more limited kinds of terms that the Uniform Commercial Code or Restatement (Second) of Contracts forbid as unconscionable.^70 Read against this history, EU data protection law views contracts in a fashion highly consistent with deeper currents in EU law.

B. The Future: Convergence or Divergence

We conclude with some thoughts about convergence and divergence. Comparative law scholars have long debated whether different legal systems are becoming more alike, and the extent to which globalization or technological developments drive this process. Writing in 1992, Colin Bennett argued that global convergence in the regulation of information privacy law had occurred “within a common technological context.”^71 More specifically, he proposed that different countries had “converged around statutory principles of data protection, but diverged in policy instruments selected to implement and enforce them.”^72

At a more granular level than Bennet and focusing on contract law in information privacy, we can identify elements of convergence and divergence between the U.S. and EU in 2015. The elements of convergence concern attempts in both the U.S. and EU to use the law to limit the bounds of contracts in order to protect consumers. As between businesses, however, both systems happily rely on contracts to bind data processors and their business associates, vendors, and outsourcers into a web of prescribed obligations.

There are also significant elements of divergence. In the EU, processing of personal data is impermissible without a legal basis. The use of contracts as a legal basis for such processing is then restricted in different ways. In some instances, for example, other legal requirements, such as "data quality," exist regardless of contractual terms. In the U.S., personal data processing is generally permissible unless a legal requirement sets limits on it. While the FTC uses privacy and security notices as part of its Section 5 authority to stop unfair and deceptive practices, the result is far from a full regime of EU-style data protection. Today, and in contrast to Bennett’s findings in 1992, the divergence seems to around both principles and policy instruments.

---

^70 For a discussion of the U.S. approach, see Cooter and Ulen, supra note 18, at 368.
^71 Colin Bennett, Regulating Privacy 150 (1992).
^72 Id. at 6.
The question for the future is whether this divergence will continue in a world dependent on international data flows, many of which involve personal data. In the U.S., the view has been that contract permits and, indeed, should safeguard the productive investment in use of information. Despite the FTC’s efforts, the U.S. legal system still is largely supportive of unifying personal information and the control of it in the hands of the large commercial entities that collect, process, and transfer such data.

VII. Conclusions
[To Follow]