

2005

Applicants Laid Bare: The Privacy Economics of University Application Files

Martin McWilliams

University of South Carolina - Columbia, mcwillmc@law.sc.edu

Follow this and additional works at: http://scholarcommons.sc.edu/law_facpub



Part of the [Education Law Commons](#)

Recommended Citation

Martin C. McWilliams, Jr., Applicants Laid Bare: The Privacy Economics of University Application Files, 34 Hofstra L. Rev., 185 (2005)

This Article is brought to you for free and open access by the Law School at Scholar Commons. It has been accepted for inclusion in Faculty Publications by an authorized administrator of Scholar Commons. For more information, please contact SCHOLARC@mailbox.sc.edu.

APPLICANTS LAID BARE: THE PRIVACY ECONOMICS OF UNIVERSITY APPLICATION FILES

*Martin C. McWilliams, Jr.**

I. INTRODUCTION

So—Princeton University’s admissions staff hacked into Yale University’s application files to get access to personal information about Yale applicants.¹ This unlikely event brings to mind the comprehensiveness of application files—a veritable one-stop-shop for those interested in applicants’ personal information. Just how private are university application files? How private should they be? The common law, supported by the law-and-economics literature, offers little protection to the privacy of personal information.² In most circumstances it allocates to those lawfully in possession of another’s personal information a right to re-employ it. A rule of disclosure is not efficient in every case, however.³ Significantly for present purposes, a rule of disclosure may well be inefficient in adhesive relationships in which willing disclosure of high-value, private facts is followed by secondary employment unanticipated by the subject. This Article addresses the privacy economics of such relationships.⁴ As an example, this Article

* Associate Professor of Law, University of South Carolina; Chair, Faculty Admissions Committee, 2002-05. Thanks to John Harvey and Ryan Langley for their patient and capable assistance. Errors are mine.

1. This event is described in many places. *See, e.g.*, Jeffrey R. Young, *Why Was Princeton Snooping in Yale’s Admissions Web Site?*, CHRON. HIGHER EDUC., July 26, 2002, at A37, available at <http://chronicle.com/free/2002/07/2002072601n.htm>; Margaret L. O’Donnell, *FERPA: Only a Piece of the Privacy Puzzle*, 29 J.C. & U.L. 679, 712-13 (2003). Sadly, this is not an isolated instance. *See infra* note 52 and accompanying text.

2. This Article addresses privacy in the sense of “control of [truthful] information concerning [an individual’s] person.” U.S. Dep’t of Justice v. Reporters Comm., 489 U.S. 749, 763 (1989). Such privacy interests are sometimes referred to as “informational privacy,” “data privacy,” and, outside the United States, as “data protection law.” Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 6 (1997) [hereinafter Schwartz, *Personal Health Care*]. Professor A. Michael Froomkin uses “informational privacy” as “shorthand for the ability to control the acquisition or release of information about oneself.” A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1463 (2000).

3. *See* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2384 (1996) (“One way to attack the problem is to set up separate rules depending on the type of information at issue.”).

4. An economics approach is chosen to avoid engagement in the “normatively charged” privacy literature based on consumer profiling. *See generally* Stan Karas, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393, 411, 415 (2002) (noting the tendency of much of the literature

will consider the secondary employment of higher-education application-file disclosures in light of two socially desirable objectives of the admission process: (1) Maximizing the content and accuracy of applicant disclosure to inform admission decisions; and (2) maximizing the number of qualified, willing applicants. Social efficiency requires pursuit of these goals at least cost.

As described below, a school's relationship with its applicants is highly asymmetrical in bargaining power and therefore highly adhesive in terms of the informational demands the school can make on applicants.⁵ As a condition of being considered for admission each applicant must permit the school to assemble a file that is chock full of the applicant's personal information. The student-records privacy rules of the Family Educational Rights and Privacy Act ("FERPA")⁶ do not protect these files because applicants are not "students" within the meaning of the statute.⁷ Nor is personal information such as that found

toward "refraction of social anxieties"). The purpose here is to show that one area of personal information accumulation is, by any measure, broken.

5. Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2078 (2004) [hereinafter Schwartz, *Property*] (characterizing a situation where individuals do not know that personal information gathered will be processed and shared as an "extreme illustration of privacy market failure").

6. 20 U.S.C. § 1232g(a)(4)(A)(ii) (2000). FERPA regulates secondary employment of student-file content and permits students access to their files, among other things. *See id.* Under FERPA's broad definition of protected "records," almost all contents of application files would be FERPA protected were applicants "students" within the statutory definition. *See* Lynn M. Daggett, *Bucking Up Buckley I: Making the Federal Student Records Statute Work*, 46 CATH. U. L. REV. 617, 624-25 (1997).

7. *See* 20 U.S.C. § 1232g(a)(6) ("For the purposes of this section, the term 'student' includes any person with respect to whom an educational agency or institution maintains education records or personally identifiable information, but does not include a person who has not been in attendance at such agency or institution."); 34 C.F.R. § 99.3 (2005) (defining "student" as "any individual who is or has been in attendance at an educational agency or institution and regarding whom the agency or institution maintains education records"). *See* Daggett, *supra* note 6, at 623 (stating that "students do not include applicants who have not attended a school," whether rejected or accepted but who do not matriculate). *But cf.* O'Donnell, *supra* note 1, at 709 n.150 (indicating that the position of the Family Policy Compliance Office, which administers FERPA under authority granted by 20 U.S.C. § 1232g(g), has been that records sent to a school by the applicant or by a testing service are not within FERPA unless and until the applicant matriculates, whereas records sent by the applicant's prior school are covered whether or not the applicant matriculates). Similarly, schools are not required to give non-students access to their files. *See id.*; *see also* Tarka v. Franklin, 891 F.2d 102 (5th Cir. 1989) (a person is not a "student" for the purpose of gaining access to his or her admission files pursuant to FERPA where his or her application was rejected and he or she merely audited classes); *United States v. Brown Univ.*, Civ. A. No. 91-3274, 1992 WL 2513, at *2 (E.D. Pa. Jan. 3, 1992) (a federal government subpoena of accepted applicants' financial aid records who elected not to attend a school did not meet FERPA's definition of "student"); *Norwood v. Slammons*, 788 F. Supp. 1020, 1026 (W.D. Ark. 1991) (an un-enrolled law student did not have standing under FERPA to object to a school's refusal to release records); *Osborn v. Bd. of Regents*, 647 N.W.2d 158, 172 (Wis. 2002) (concluding that production of redacted records is not prohibited by FERPA, so that the issue of whether application records are protected by FERPA need not be reached);

in application files protected by any general privacy norm.⁸ How is the privacy of application-file content regulated, and why? Judge Richard Posner has aptly described attempts to apply analytical structure to privacy as “a puzzle.”⁹

This Article does not attempt a statement of a broad privacy right informed by a general normative interest, although there are normative aspects to what it does investigate. Rather, the point here is to evaluate the utility of allocation of the value of personal information in a strongly adhesive regime in which the personal information is solicited, and willingly disclosed, for a particular purpose.¹⁰ I conclude that the present admissions-information regime is inherently inefficient. It is costly to applicants because they do not know (or even know that they need to know) the value of what they are required to surrender, and therefore lose the opportunity to extract fair value for surrendering it. It is risky to applicants because they do not know (or have any way of learning) to what further and costly uses such information may be put.¹¹ At the same time, the current regime is potentially costly to schools in terms of their admissions goals: If applicants knew, or suspected, that personal information revealed in application files might be put to uses they did not anticipate—“excessive secondary employment”¹²—the quantity and

Vandiver v. Star-Telegram, Inc., 756 S.W.2d 103, 107 (Tex. App. 1988) (a recruited athlete’s records were not “student” records under the state’s open records law because of a lack of proof that the athlete enrolled at a school).

8. See, e.g., Vera Bergelson, *It’s Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 383 (2003) (“Under the current law, individuals neither own their personal information, nor have a recognized privacy interest in it.”); *Id.* at 403 (“Currently, neither property nor torts theory recognizes individuals’ rights in their information.”); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1284 (2000) (dossiers of personal information “may be used, sold, published . . . [and] that’s completely legal”); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1138 (2000) (“when the owner of a property right sells her interest to another person, that buyer can freely transfer to third parties” the interest so acquired); Craig D. Tindall, *Argus Rules: The Commercialization of Personal Information*, 2003 U. ILL. J.L. TECH. & POL’Y 181, 187 (2003) (“Short of some highly injurious or offensive use, corporations can use personal information about customers in almost any manner they believe might be profitable.” (citing RESTATEMENT OF TORTS (SECOND) 652B-652E (1977))).

9. RICHARD A. POSNER, *THE ECONOMICS OF JUSTICE* 309 (1981).

10. There are many such regimes, which run the range from purchases done over the Internet, enrolling in supermarket and other retail discount card programs, participation in religious organizations, involvement in community associations, participating in events for charity (including making contributions), to simply joining a health club. Characteristic is a perceived high level of private and social utility in an enterprise with admission based on a take-it-or-leave-it set of criteria, including disclosure of personal information.

11. Where a group of parties does not know to what use their personal information will be put, the relationship takes on the characteristics of a “monopoly equilibrium.” Schwartz, *Personal Health Care*, *supra* note 2, at 49.

12. See *id.* at 31 (“An excessive disclosure norm for certain kinds of information will distort

accuracy of disclosed information might well decline, and some students might not apply at all. Finally, because applicants persistently sell their personal information too cheaply to schools, and because the schools do not bear the risk of cost attributable to excessive secondary employment of the applicants' information, the schools, acting rationally, are incentivized to under-invest in application-file security. Schools choosing to employ applicant-file information to make secondary-employment gains will free ride.

Applicants, then, are not able to internalize the benefits of the information they provide schools, but do bear the cost of furnishing file information and the risk of excessive secondary employment of that information by the schools. Higher cost will reduce quality.

I suggest in what follows that efficiency would best be served by reversing the present default rule, which permits secondary disclosure, in favor of a coercive default rule of non-disclosure, stimulating schools to surrender their informational advantage concerning secondary employment and security of application files.

Part II describes the economics of application files and explains the justification for the extreme adhesiveness of the process. Part III discusses the limits of the efficiency of the present application-information regime. Part IV reviews the current state of protection of personal information, concluding that application files receive little legal protection. Part V proposes that efficiency requires a new, coercive default rule to regulate adhesive relationships by shifting cost to the institutional collectors of personal information. This Article concludes that a rule of disclosure-based self regulation is more efficient than the present default disclosure rule, and more congruent with society's perceived, but indistinct, privacy norm.

II. THE ECONOMICS OF APPLICATION FILES: LAYING THE APPLICANT BARE, FOR GOOD REASON

Application files are a gold mine of personal information, much of which, in other contexts, applicants would be reluctant to reveal. As one observer has noted, individuals are best able to control personal information by not revealing it in the first instance,¹³ but higher-education applicants do not have this option. The admissions process strictly requires, as a condition of entry into the process, the disclosure

or eliminate the kinds of personal information [the subjects] share in future transactions . . ."). In this Article "excessive secondary employment" will be used to describe secondary employment, the cost or riskiness of which exceeds the subject's gains from the initial disclosure of information.

13. See Froomkin, *supra* note 2, at 1464.

of personal information sufficient to lay the applicant absolutely as bare as possible. Schools require this for good reasons, but also simply because they can; the process is not regulated except by the schools themselves. This extremely adhesive arrangement will tend toward efficiency at the level of primary employment, as this Part will describe, but secondary employment, intended or unintended, can render the process inefficient, as explained in Part III.

A. *What's at Stake?*

While the applicant is the subject of almost all of the information in an application file, most of that information is provided by others, including the applicant's former educational institutions, present and past employers, writers of letters of recommendation, interviewers, admissions committee members, admissions staff, data assembly services, law enforcement agencies, and so on.¹⁴ A complete file contains a comprehensive record of the applicant's experience in higher education and considerable information about the applicant's personal life, including undergraduate grade point average ("GPA") and class standing, transcripts, admissions-test scores present and past, disclosure and explanation of university discipline records (student disclosures in this respect are double-checked with their colleges) and any brushes with the law (not limited to criminal records—typically, any arrest beyond a routine traffic violation must be included, whatever the outcome), military-service information (such as whether a person's discharge was or was not honorable), letters of "recommendation" (sometimes negative), the applicant's Social Security number, the applicant's addresses and telephone numbers and often those of family members, occasionally a photocopy of a personal check (with the applicant's bank account and routing numbers on it), disclosure of membership in organizations, essays that are often highly personal, faculty vote sheets with comments, interview notes, the admissions decision itself, vote sheets and decisions from any unsuccessful previous attempts at admission, information about any health or disability issues,¹⁵ the names of other schools to which the applicant has applied, where the applicant has been accepted and at what schools the applicant has put down a seat deposit, and miscellaneous information of all kinds about an applicant

14. See Michael A. Olivas, *Higher Education Admissions and the Search for One Important Thing*, 21 U. ARK. LITTLE ROCK L. REV. 993, 994-95 (1999).

15. See *id.* Health and disability issues are regulated under the Individuals with Disabilities Education Act ("IDEA") and regulations thereunder. See, e.g., 20 U.S.C. § 1400 (2000). Because the IDEA is designed to work in parallel with FERPA, see 20 U.S.C. § 1417(c) (2000), it is not discussed individually in this Article.

that finds its way into the file. Much of this material is required by the school and much that is not required is volunteered by the applicant or other contributors. The result overall is that the applicant, in the interest of an informed admissions decision, is laid bare (or, at least, so the admissions committee intends). And of course the applicant bears almost all of the cost of this compilation.

Of particular significance is that all of this information is *in one place*, furnishing a one-stop-shop for those with an interest in an applicant's personal information. And that place is regulated only by the school itself.

The admissions procedures of institutions of higher education are perfectly adhesive in that they give applicants no choice but to subject themselves to the fixed conditions of application, including that applicants lay themselves bare as they run what the Supreme Court has characterized as "the gantlet" of admissions.¹⁶ This self-revelation is multiplied, of course, by the tendency of applicants to apply to more than one school. A recent study shows that law school applicants, for example, apply on average to at least four law schools, and the trend is headed upward.¹⁷ On average, then, each applicant is subject to multiple revelations, each within the context of whatever self-regulatory approach each school applied to has chosen to adopt.

B. *The Admissions Efficiencies of Primary Disclosure.*

Higher-education applicants are laid bare for good reasons of accuracy, comprehensiveness, and, in the case of professional schools, professional ethics. As this Part will explain, disclosure is efficient, and privacy is inefficient, so far as the primary employment of application information is concerned.

16. *DeFunis v. Odegaard*, 416 U.S. 312, 319 (1974).

17. The Law School Admission Council's report entitled "National Applicant Trends—2004" notes that:

[A]pplications per applicant ranged from 4.8 to 4.9 during the 5-year period from 1991 through 1995 and between 4.5 and 4.7 during the 5-year period from 1996 through 2000. For 2001 there were 4.7 applications per applicant, but by 2004 the number had increased to 5.5 It seems likely that this ratio will remain high as long as applicants perceive that volumes are remaining high.

LAW SCH. ADMISSIONS COUNCIL, NATIONAL APPLICANT TRENDS—2004, at 1 (2004), *available at* <http://www.lsacnet.com/lsac/data/National-Applicant-Trends.pdf>. Additionally, in a brochure copyrighted in 1996, the State Bar of Arizona specifically advised prospective law students to apply to multiple law schools. The Arizona Bar continues to publish this recommendation on its official website at <http://www.azbar.org/PublicResources/Brochures/career.asp> (last visited Feb. 11, 2004). The online brochure states that "[n]o two schools apply the same criteria equally; it therefore is important to apply to more than one school." *Id.*

1. File Accuracy and Comprehensiveness: Privacy as Inefficient Secrecy

Personal information is the basis of countless privately and socially beneficial decisions “routinely” entered into.¹⁸ Were the common law to protect a right to the privacy—“secrecy”—of such information, such decisions would be less efficient across the board, for three reasons. First, the transaction cost (including information cost) of negotiating around a default rule of privacy would render impracticable many transactions that would otherwise be socially beneficial.¹⁹ Second, as the relevant literature explains, individuals rationally attempting to maximize self-interest will, where possible, conceal or distort personal information to their advantage, leading to inaccurate, and therefore inefficient, decision-making.²⁰ Finally, the subject of personal information—the applicant in this context—is most likely to be the lowest-cost provider of any personal information that is required to permit a transaction to go forward. Accordingly, a rule enabling privacy would increase information cost as an aspect of transaction cost across the board. Nor would privacy, applied in routine cases, avoid cost to subjects of personal information sufficient to justify the loss of otherwise socially valuable transactions.²¹

The inefficiency of privacy is directly relevant to applications because the adhesive nature of the process mitigates an important information asymmetry favoring the applicant. Schools begin the application process with virtually no information about their applicants. Each applicant is therefore positioned to exercise control over their personal information for the very purpose of distorting the admissions committee’s evaluation of the applicant, leading to inefficient admissions decisions.

The effect of conditioning entry into the admissions process on full disclosure is that the school is able to obtain an account of the applicant’s qualifications that is as complete and accurate as possible. Less information reduces the admissions committee’s ability to draw distinctions among applicants and therefore results in more uniform

18. See, e.g., Bergelson, *supra* note 8, at 381.

19. “Privacy” in this sense is control of personal information, particularly its secondary employment. Professor Schwartz refers to privacy in this sense as “information privacy.” Schwartz, *Property*, *supra* note 5, at 2058.

20. See Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 397-403 (1978) [hereinafter Posner, *Right of Privacy*] (describing “privacy” as a means of concealing adverse personal information).

21. Cf. Karas, *supra* note 4, at 416 (“There are no adverse consequences from routine data collection, except for the greater volume of junk mail.”).

treatment.²² Sorting among applicants becomes less efficient in terms of bringing to bear the particular school's admissions goals, whatever they may be in particular cases. Less particularized information renders the admissions decision more difficult (costly), and more random, increasing the likelihood that admissions decisions will be ill-informed (another cost). Reducing the amount of particularized information makes it more likely that resources invested in the school will not be applied according to whatever the applicable social goals might be in particular cases, a social cost. Less information, in other words, creates a market for lemons, with consumer valuation tending toward an average.²³

Efficiency in this sense lies in minimizing the sum of the cost of information-gathering and of making bad decisions. The more information about an applicant that is gathered by the admissions process, and the lower the cost to the school, the more efficient the process will be. Each additional piece of information gathered by the school renders the school marginally more observant in making its determinations, rendering the market in applications marginally more efficient. High quality applicants ("peaches")²⁴ are more likely to be identified by the school and rewarded (by acceptance and perhaps also by financial assistance), making the peaches more likely to apply.²⁵ More information tends toward optimal results, benefiting the peaches and the schools.

On the presumption, then, that admission is based upon particularized qualifications, the more particularized the scope of inquiry, the better. In my role as Admissions Chair at the law school where I teach, I tell people, "The more we know about an applicant the better we like it," and that is good economics.

2. The Efficiency of Willing Disclosure

Willingness of exchange suggests that each party receives something they value more highly than the thing they are exchanging,

22. Cf. George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 630 (1980) ("When it becomes more difficult to measure differences among individuals, their treatment becomes more uniform" with efficiency suffering as descriptions tend toward an average).

23. See generally George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECON. 488 (1970). Professor Akerlof's article famously articulates the economics of such circumstances in terms of the market for defective cars ("lemons"). See *id.* at 489. Ill-informed consumers will willingly pay an average price for defective cars but, because they are ill-informed, no premium for above-average ones ("peaches"). There is accordingly no market for peaches.

24. *Id.*

25. See generally *id.*

and this is efficient²⁶—indeed, it lies at the heart of the concept of economic efficiency.²⁷

Application file content is willingly provided and the accumulation of personal information from collateral sources is willingly permitted. This means that to the applicant, keeping the personal information in the file private is worth less than the opportunity to be considered for admission. Clearly the applicant values the opportunity to be evaluated for admission more highly than privacy. Every applicant makes this evaluation. This must be true, or the applicant would not agree to be subject to the highly adhesive, and intrusive, gantlet of admissions.

3. Professional Ethics

Finally, there is the professional ethics issue. The law school application process, for example, is the first filter in the assessment of a prospective lawyer's character and fitness for the practice of law. Certainly it is much harder to get admitted to my law school if an applicant's file reflects character-and-fitness issues. This is exactly the kind of information that law-school admissions committees want to be able to take into account and that applicants, rationally managing the stream of information about themselves, might prefer not to share. In this respect, the law-school admissions process may differ, at least in degree, from other higher-education admissions processes.

4. Summary of Part II

So far as first-level employment (that is, the admissions process itself) is concerned, cost to the applicant is assessable, consisting almost entirely of the out-of-pocket cost of the process and the "pure privacy preference"²⁸ of keeping personal information secret from those involved in the process. Those who apply have determined that the benefit of entering the admissions process is worth more to them than these costs. Both school and applicant are better off than before. At the

26. See Richard A. Posner, *The Ethical and Political Basis of the Efficiency Norm in Common Law Adjudication*, 8 HOFSTRA L. REV. 487, 488-89 (1980) [hereinafter Posner, *Common Law Adjudication*] (examining different perspectives on meaning of efficiency, including Pareto and Kaldor-Hicks efficiency).

27. See, e.g., RICHARD A. POSNER, *ECONOMIC ANALYSIS OF LAW* 13 (6th ed. 2003) [hereinafter POSNER, *ECONOMIC ANALYSIS*] (viewing efficiency as wealth-maximizing in a Kaldor-Hicks sense, as this Article will do).

28. Murphy, *supra* note 3, at 2393-96. Privacy advocates put high value on the pure privacy preference. See, e.g., Tindall, *supra* note 8, at 191 (2003) (rather than creating "economic damage . . . the harm visited upon consumers by a loss of privacy is more emotional—a feeling of powerlessness and loss of personal security."); Edward J. Bloustein, *Privacy is Dear at Any Price: A Response to Professor Posner's Economic Theory*, 12 GA. L. REV. 429, 447 (1978).

first level of disclosure, then, an unencumbered flow of private facts into application files through a highly adhesive process is appropriately congruent with the general economic preference for a rule of disclosure. Each item of information that enters an application file makes the admissions decisions marginally more efficient. The school, as the consumer of the information, is made marginally more observant. Across the board, the socially beneficial application process is enhanced.²⁹ In the present regime, this view prevails. Accordingly, at the level of first employment it is efficient for applicants to be laid as bare as possible. Whether it is efficient at the level of secondary employment is a very different issue, discussed in Part III.

III. LIMITS ON THE EFFICIENCY OF A RULE OF DISCLOSURE IN ADMISSIONS FILES

Part II concludes that, at the primary level of employment of applicants' personal information, privacy is inefficient, and disclosure efficient. This Part discusses the likelihood that the very characteristics that make the highly adhesive nature of the admissions process efficient at the primary level of employment risk inefficiency when subjected to the common-law default rule of disclosure in secondary employment. This Part discusses relevant cause and effect, including unanticipated and excessive secondary disclosure, applicants' inability to value their personal information, and costs to schools.

A. *The Secondary Employment of Personal Information*

According to the efficiency-informed default rule, private facts willingly disclosed fall within the general conclusion of the case law, supported by the law-and-economics literature, that cheaply available, accurate, personal information tends to lower transaction cost and enhances accurate decision making, while keeping information private tends to have the opposite effect.³⁰ Economics explains that the secondary employment of personal information can create social value,³¹

29. Maximizing the information about a particular applicant might well reduce that applicant's chances of admission. Because that party to the admissions transaction is not made better off, the efficiency described here would be Kaldor-Hicks, increasing the economic value of social resources despite leaving some individuals worse off. See POSNER, *ECONOMIC ANALYSIS* *supra* note 27, at 13.

30. See Murphy, *supra* note 3, at 2382.

31. See, e.g., Posner, *Right of Privacy*, *supra* note 20, at 394. See also Bergelson, *supra* note 8, at 403. Professor Bergelson notes the "view" that "personal information is no one's until collected," analogizing this to the rule that wild animals belong to no one until captured. *Id.* at 403 (citing *Pierson v. Post*, 3 Cai. R. 175 (N.Y. Sup. Ct. 1805)). Professor Bergelson's observation is

a phenomenon empirically demonstrated repeatedly.³² Once personal information has been lawfully transmitted by its subject, its secondary employment by the new possessor continues to be efficient so long as it creates value greater than any resulting cost to the subject. Judge Posner's paradigmatic example describes the sale by magazines of their subscription lists.³³ Lists of subscribers' addresses are "generally worth more to the purchasers than being shielded from possible unwanted solicitations is worth to the subscribers."³⁴ The transaction cost of obtaining consent of the subscribers is "high relative to the value of the list," so consent is not required, putting the list into the hands that value it most at least cost.³⁵ Judge Posner concludes that "we should assign the property right [of secondary employment] to the magazine; and the law does this."³⁶ Efficiency is served by transferring truthful personal information, lawfully obtained, into hands in which it is more highly valued than by its subjects, and where that value can be extracted at a cost low enough to result in a net social gain. This example is meant to demonstrate that, as a general proposition relating to personal information, social efficiency lies in a rule of disclosure.

Supporting this conclusion of economics is the default rule that the parties to a transaction have the right to re-employ information acquired in the transaction.³⁷ To avoid this result, the parties must bargain away

paralleled by the phenomenon of economics, that information has zero value in the hands of its subject, obtaining value only in the hands of someone who values it at greater than zero. *See also* Tindall, *supra* note 8, at 182, 192; Kalinda Basho, *The Licensing of Our Personal Information: Is it a Solution to Internet Privacy?*, 88 CAL. L. REV. 1507, 1514 (2000).

32. *See, e.g.*, William J. Fenrich, Note, *Common Law Protection of Individuals' Rights in Personal Information*, 65 FORDHAM L. REV. 951, 956 (1996) ("The annual market for mailing lists alone, without factoring in sales attributable to their use, has been estimated at approximately \$3 billion."). *See also* Bergelson, *supra* note 8, at 382 n.8 (citing a study estimating that the "value of each name is typically worth 3 to 20 cents each time it is sold"); Walter W. Miller, Jr. & Maureen A. O'Rourke, *Bankruptcy Law v. Privacy Rights: Which Holds the Trump Card?*, 38 HOUS. L. REV. 777, 779 (2001) (noting that in many cases, an e-commerce company's most valuable asset is its customer database).

33. *See* Posner, *Right of Privacy*, *supra* note 20, at 398 (citing *Shibley v. Time, Inc.*, 341 N.E.2d 337 (1975)).

34. *Id.*

35. *Id.*

36. *Id.* (citing *Shibley*, 341 N.E.2d at 337). *Accord* Avrahami v. U.S. News & World Report, Inc., No. 95-1318, 1996 WL 1065557, at *6 (Va. Cir. Ct. June 13, 1996) ("no property right" in names used in making purchases); Bergelson, *supra* note 8, at 403-04.

37. *See, e.g.*, Fromkin, *supra* note 2, at 1502 ("[B]oth sides to a transaction generally are free to sell details about the transaction to any interested third party."); Samuelson, *supra* note 8, at 1131 ("the traditional view in American law has been that information as such cannot be owned by any person. . . . Many examples illustrate that the law does not generally recognize the legal right of individuals to control uses or disclosures of personal data."). Professor Samuelson considers this to be a disadvantage of treating personal information as property. *See id.* at 1138.

the default rule, as by entering into a non-disclosure agreement. In many cases, such as in the example of magazine subscriptions, to bargain away the default rule would be so costly as to exceed the value of the transaction, so that if bargaining were required, the socially valuable transaction would not occur.

In the case of application files, neither the common law nor government regulation contradicts such a default rule.³⁸ Nor, as a practical matter, can the default rule be contracted around, due to the combination of prohibitive transaction cost and the strongly adhesive applicant/school relationship. Accordingly, the contents of application files are not protected from opportunistic secondary employment, especially if they can be employed to achieve gains.³⁹

As detailed above, application files contain information of much higher value to the subject, and to others, than a mere subscription address. Such information, revealed to schools, may pass on into the datasphere, to be accumulated, catalogued, and re-employed in various ways to the advantage of parties other than applicants and schools. The applicants' personal information is subject to becoming the property, in effect, of strangers, and used for the benefit of strangers.⁴⁰ This can happen either purposefully as the school exercises its "Posnerian" property right in the information, or inadvertently through file leakage. There is incentive for this to happen because of the demand for personal information and fast-growing and low-cost transmission of such information in rapidly developing markets.⁴¹

The foregoing scenario can be efficient if it creates social value. In the hands of a school, its employees, and others who are able to obtain

38. In terms of state regulation, New York is the only state that appears to have addressed the issue of application file privacy directly. In considering a Freedom of Information Act ("FOIA") request, New York's Committee on Open Government interpreted that state's FOIA statute to allow the information officer to deny access to portions of a law school applicant's file in order to prevent an unwarranted invasion of privacy. *See* COMM. ON OPEN GOV'T, FOIL-AO-9544 (June 18, 1996) (citing N.Y. PUB. OFF. LAW § 87 (McKinney 2003)). Importantly, however, this decision was discretionary under the statute, not mandatory. *See id.*

39. *See infra* text accompanying note 156; Froomkin, *supra* note 2, at 1502.

40. *Cf.* Schwartz, *Property*, *supra* note 5, at 2066 (observing that once personal information is gathered by online "spyware," it is subject to repeated re-employment).

41. *See, e.g.*, Tindall, *supra* note 8, at 182 ("[T]he collection and use of personal information [in the market] . . . will unquestionably continue at an ever-increasing rate."). *See also* Karas, *supra* note 4, at 395 (describing the probable rapidity of growth of personal information databases); *Id.* at 399-400 (describing the present as an "explosive time" in data marketing); Samuelson, *supra* note 8, at 1126 ("The market incentives for firms to collect and process personal data are very high."); *Id.* at 1132-33 ("Many firms collect and process personal data because of its value and because information technology makes the collection and use of such data so much easier and cheaper. They also do so because they are not forced to internalize the societal costs of private sector processing of personal data.").

file access, application information can have value for purposes other than admissions. At one level, admission to an institution of higher education is a scarce resource. Information about its allocation, and influence in its operation, has value that can benefit anyone able to obtain file access.

At another level, the default rule of disclosure permits schools to employ application-file information opportunistically. Certainly schools secondarily employ it to inform the admissions process generally, as opposed to its use in specific cases, to perform empirical analysis, for example. Other less obvious examples include the use of file content in school publicity,⁴² or use by the development office to identify applicants of interest to fund-raising targets or persons of political influence. At yet another level, schools literally could sell application file information. If magazines can retail subscribers' addresses, there is little to keep schools from doing similar marketing.⁴³ I would argue that all of these uses create gains for the school. Externalization of the costs of operating a public institution is socially valuable.

In summary, an argument can be made that secondary employment of application-file information by schools is socially beneficial. The efficiency of secondary employment of personal information should be tested, however, against cost to the subject, the value to the subject of not having the information secondarily employed, and against its tendency to discourage socially beneficial actions.⁴⁴ This is discussed next.

B. Potential Secondary Employment Costs to Applicants

Secondary employment of personal information in application files is effectively a windfall for the school that chooses to employ the information opportunistically. The school obtains, in addition to the information it requires for admissions purposes, the opportunity of

42. For example, the admissions offices of universities around the country publicize the scores and grades of applicants who applied to their programs even if they were not admitted. This practice does not identify each applicant by name, but does constitute disclosure of the applicants' personal information from which the schools are obtaining a benefit (by portraying the university in a positive light for admitting only the upper tier of the students who applied for admission).

43. Cf. Robert Gellman, *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete*, at 9 (2002), <http://www.epic.org/reports/dmfprivacy.html> (describing how U.S. Bancorp sold customer information to a telemarketing firm, including credit card numbers, credit limits, and Social Security numbers, consequently was sued by the Minnesota Attorney General alleging privacy breaches, and ultimately settled without admitting wrongdoing). Similar cases are described in Froomkin, *supra* note 2, at 1473-74.

44. See Posner, *Right of Privacy*, *supra* note 20, at 397.

secondary employment unanticipated by the applicant. In a sense, then, the schools are not paying the full cost of the personal information they obtain.⁴⁵ The availability of information at less than true cost will result in underinvestment in applicants' privacy preferences, such as file security and limitations on secondary employment.⁴⁶ It should also result in high investment in obtaining file information, but the present regime allocates most of the cost of assembling the file to the applicant. This lowers the cost of opportunistic secondary employment by the school. Indeed, as the cost to the school of assembling the file is attributable to the primary employment (the actual admission decision), secondary employment is costless to those schools deciding to use it opportunistically. Self-regulation of secondary employment permits such free riding, and likely does so in contradiction of the expectations of applicants. In short, then, schools internalize gains from primary and secondary employment of application-file information but externalize the costs of obtaining the information. Cost to the applicant, including information cost, plus the adhesive nature of the process, minimizes bargaining, probably to zero. This systematizes an incentive to "overuse" such information.⁴⁷

In contrast to the information windfall allocated to the schools, the rule of disclosure dramatically allocates to the applicants the risk and cost of secondary employment, whether purposeful or inadvertent. It is possible, of course, for secondary employment of personal information to be costless, or virtually costless, to subjects; consider, for example, Judge Posner's magazine subscriptions. Countless consumer transactions in which consumers part with bits of personal information fall into this category.⁴⁸ Secondary-employment cost to the subject can, however, exceed the subject's gains from the initial, willing disclosure (hereinafter "excessive secondary employment").⁴⁹ Excessive secondary employment is almost always unanticipated, so such cost is not taken into account by the subject in making the initial disclosure decision. In light of the highly significant personal-information contained in application files, secondary employment, unanticipated, may well be

45. See Schwartz, *Property*, *supra* note 5, at 2079 (describing various market failures of the information markets).

46. *Cf. id.*

47. *Cf.* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 8 (1998).

48. See, e.g., Tindall, *supra* note 8, at 191 (collection and re-employment of consumer marketing information rarely causes material "economic damage").

49. See Schwartz, *Personal Health Care*, *supra* note 2, at 31 ("An excessive disclosure norm for certain kinds of information will distort or eliminate" future sharing of information by the subject).

excessive.

Cost allocated to applicants will include short-term incremental cost, the loss of the pure privacy preference at the level of secondary employment, the out-of-pocket cost of the application—testing, fees and so on—and the private costs of undesirable revelation of the application itself to family or employers. While Kaldor-Hicks analysis would suggest that such costs are subsumed by the social benefit of the availability of accurate information, such private costs are nevertheless allocated to each applicant at that applicant's particular marginal cost. This can be far higher than market value, an adversely discriminatory effect.

Included in incremental cost to applicants will be cost of loss of control of personal information, an issue that has been catalogued in many places.⁵⁰ For present purposes let it suffice to say that it can include junk mail, spam and other internet costs, and exposure to telemarketing.⁵¹

Also allocated to the applicant will be high, long-term risk (e.g., identity theft) associated with having so much potent personal information gathered in one, self-regulated place.⁵² As Professor Samuelson has observed, if your car is stolen you can buy another, but once your personal information enters the datasphere, replacement privacy is not available for sale.⁵³ Long-term risk in this context is particularly coupled with inadvertent secondary employment—inappropriate file access or hacking-in to electronic files.

In addition to purposeful secondary employment of applicant information by the school, failure by the school to limit application file access may result in unintended information leakage costly to the applicant, either by unauthorized or inappropriate physical access or by such methods as hacking into electronic files. Indeed, evidence of “systematic . . . unauthorized” access to student files is one of the

50. See, e.g., Gelman, *supra* note 43, at 18-28.

51. See *id.*

52. This is a rapidly growing problem. For example, in less than two weeks in the spring of 2005, three universities in California experienced security breaches concerning the personal information of approximately 180,000 current, former, and prospective students. Tom Zeller, Jr., *Some Colleges Falling Short in Data Security*, N.Y. TIMES, Apr. 4, 2005, at C1. The security breach affecting UCLA-Berkeley involved access to the names and Social Security numbers “of nearly 100,000 people—mostly graduate school applicants.” *Id.* The University of Southern California was also hit a few weeks later, when the personal information of 270,000 “current and former applicants” was compromised by a hacker who broke into a university database. Dan Carnevale, *Computer Break-In at U. of Southern California Prompts Warning to 270,000 Applicants*, THE CHRON. HIGHER EDUC., July 22, 2005, at A24.

53. Samuelson, *supra* note 8, at 1145 n.110.

reasons FERPA was enacted.⁵⁴

Adhesive self-regulation makes possible opportunistic secondary employment by other persons at the school who manage to gain file access. For example, a school-regulated environment may allocate opportunity to school staff to use applicants' personal information for their private benefit, such as by currying favor with a spouse's boss whose child is an applicant. Such uses are not unlawful; they are unregulated. The cost of inadvertent secondary employment is not borne by the school, but by the applicant.

C. Cost to Schools

While the self-regulated admissions regime, in the pursuit of a least-cost approach to information collection, allocates most incremental cost and virtually all risk to the applicants, the regime is inherently costly to schools in terms of their admissions goals and reputation.

1. Costliness in Terms of Admissions Goals

Secondary employment may perversely compromise desirable social objectives gained by primary employment. In the case of higher-education applications, these objectives will include maximization of disclosure, its accuracy, and maximization of the number of qualified applicants. If subjects know or suspect that their willingly disclosed personal information is subject to excessive secondary employment they may distort their primary disclosure, or not make it at all.⁵⁵ This result is inefficient in many contexts in which the costs of distortion or lost transactions may exceed gains. A recent study has concluded that

54. See O'Donnell *supra* note 1, at 681 ("There has been clear evidence of frequent, even systematic . . . unauthorized collection of sensitive personal information and the unauthorized, inappropriate release of personal data" about students by schools). FERPA prohibits both access to student records by anyone (including school employees and officials) who lacks a "legitimate educational interest" in the records, see 20 U.S.C. § 1232g(b)(1)-(1)(A) (2004) and oral disclosure of information contained in the records, see 34 C.F.R. § 99.30(a)-(d) (2005) (defining "disclosure" as not limited to access to the records themselves). FERPA has been construed to require care to avoid inadvertent inappropriate access. See Daggett, *supra* note 6, at 632.

55. See Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting*, in *THE ECONOMICS OF INFORMATION SECURITY 5* (Jean Camp & Stephen Lewis eds., 2004), available at http://www.heinz.cmu.edu/~acquisti/papers/acquisti_grossklags_eis_refs.pdf [hereinafter Acquisti & Grossklags] (noting the consumer "defensive strategy" of falsifying information or of not completing transactions at all, in order to avoid accurate disclosure). Cf. Schwartz, *Personal Health Care*, *supra* note 2, at 31-34 (noting that unrestricted disclosure of AIDS patients' information by physicians to insurance companies has led to less than forthright statements from suspecting patients and growth of a strong market for anonymous testing on the one hand, and, on the other, significant loss to insurance companies due to inaccurate physical exam reports).

“perceived privacy and perceived security [play] a role in the nature and type of information that a consumer is willing to share with a vendor,” and that “if consumers perceive the sharing of . . . information to be not so secure or private, they are unlikely to allow the acquisition and use of this information.”⁵⁶ For example, awareness of secondary employment might discourage medical patients from disclosing information about communicable disease to their physicians.⁵⁷ In the admissions context, schools incurring cost in terms of admissions goals must therefore choose among more costly methods of obtaining the required information, the cost of making bad decisions, and the loss of beneficial transactions.

Accordingly, if applicants learn of or suspect excessive secondary employment they may diminish the content and accuracy of application information, and perhaps not apply at all. This represents the loss of a socially beneficial activity, against which any gains of secondary employment should be balanced.⁵⁸

Legal cost can also result from failure to pay attention to privacy concerns. Private and public lawsuits based on privacy issues are common.⁵⁹ Clear, expectation-based rules have been shown to minimize such litigation.⁶⁰

2. Costliness in Terms of Reputation

Trust has high value in the information markets. Economic research shows that lack of trust in vendors will lower consumer willingness to conclude transactions, and that privacy and security of personal information are key elements of trust.⁶¹ In the admissions context, this supports the suggestion that applicants’ lack of trust in a school’s application-file system will degrade application-file content and reduce the number of applications.

Accordingly, secondary employment, even if not otherwise

56. Rammath K. Chellappa, *Consumers’ Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security* 35-36, (Univ. S. Cal., Working Paper), available at <http://asura.usc.edu/~ram/rcf-papers/sec-priv.pdf>. See also Acquisti & Grossklags, *supra* note 55, at 2 (“On the Internet, sales for billions of dollars are said to be lost every year because of information security fears.”).

57. See Schwartz, *Personal Health Care*, *supra* note 2, at 31-33.

58. See *id.*; see also Richard A. Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405, 408 (1981) [hereinafter Posner, *Economics of Privacy*].

59. Gellman, *supra* note 43, at 16.

60. See *id.*

61. See Chellappa, *supra* note 56, at 34-36; Jeff Sovern, *Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1065 (1999) (citing a poll showing that “thirty percent of Americans decided against applying for jobs, credit, or insurance because they did not want to reveal certain information about themselves”).

excessive, may entail cost to the school in terms of the appearance that the admissions process is not fair or that application information is not adequately safeguarded by the school. Unintended secondary employment of disclosure may occur through lack of care by the school in controlling accidental or purposeful file access by third parties, an increasing issue as information collections become increasingly electronic.⁶² Even if such inadvertent secondary employment does not impose cost on the applicant, if suspected or discovered by the applicant it would tend to degrade the content of information submitted by the applicant or third persons, and should entail a reputation cost to the school.

3. The Risk of Governmental Regulation

Where forces such as those described in the preceding sections cause private and common-law regulation to tend to inefficiency in persistent patterns, a case is stated for some form of government regulation.⁶³ This is a significant and potentially very costly risk run in highly adhesive situations that fail properly to self-regulate. FERPA and the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) are examples. Government regulation would be costly to schools in real terms and in terms of admissions goals.

Schools’ admissions goals are highly eccentric, far too subjective to be suitable for one-size-fits-all regulation. The legislative absence of application files from FERPA suggests a conclusion that overall, the systemic costs of governmental regulation would be higher than the privacy gains to applicants. It reflects a decision to let the admissions process self-regulate in light of the extreme subjectivity of the admissions process and the eccentric values of schools.⁶⁴

FERPA-type governmental regulation allocates significant administrative cost to schools.⁶⁵ Staff time and other resources are

62. Consider, for example, the opening scene of this Article: The Princeton admissions department famously gained access to Yale’s digital admissions files using applicants’ personal information from Princeton’s own application files. *See supra* note 1 and accompanying text.

63. Indeed, statutory intervention has been called for in both the scholarly literature, see, for example, Schwartz, *Property*, *supra* note 5, at 2100, 2127-28, as well as in practice. *See* S. 116, 109th Cong. (2005) (introduced by Dianne Feinstein); H.R. Res. 1848, 108th Cong. (2003) (introduced by Robert E. Andrews).

64. The Supreme Court has acknowledged the broad range of discretion accorded to university admissions committees. *See, e.g.*, *Grutter v. Bollinger*, 539 U.S. 306, 329-30 (2003); *Regents of Univ. of Cal. v. Bakke*, 438 U.S. 265, 314 (1978) (Powell, J., referring to the “range of factors a university properly may consider”); *DeFunis v. Odegaard*, 416 U.S. 312, 325 (1974) (Douglas, J., dissenting) (“the educational policy choices confronting a university admissions committee are not ordinarily a subject for judicial oversight”).

65. *See* Daggett, *supra* note 6, at 660-62 (discussing “burdens . . . imposed” by FERPA).

required for compliance and monitoring, and systems must be appropriately adjusted.⁶⁶ As the record of decided cases shows, considerable resources must be expended on legal advice and lawsuits. One commentator has observed that the “greatest burden [FERPA] places on schools is dealing with its conflicts with other laws.”⁶⁷ It has been noted that lawyers representing colleges and universities spend “an inordinate amount of time deciphering” FERPA.⁶⁸ This is partly because FERPA, like most statutory schemes, is fixed in terms of its written provisions which in turn were limited to what seemed possible and desirable at the time of its passage. Accordingly, there are gaps in FERPA, emphasized by the lack of clarity of the relevant United States Supreme Court decisions.⁶⁹

D. Summary

This Part has explained that secondary employment of application-file information by schools can create value, much like the subscription lists exploited by Judge Posner’s magazine publishers. The resulting externalization of cost will be socially efficient so long as cost to the applicant—both actual, and perceived by the applicant—is sufficiently low. But secondary employment can be excessively costly to both applicant and school. Indeed, actions by a school that degrade information provided by applicants will force the school to choose between the costs of doing their own research or the risk of making bad decisions. Excessive secondary employment proceeds directly from the common-law default rule of disclosure. This demonstrates a tension in the rule and suggests that a perfectly general rule of disclosure is not efficient across the board. Indeed, in the admissions context a rule of disclosure allocating a right of secondary employment may never be efficient, on account of the information asymmetry disadvantaging the applicants. The next Part describes the failure of the common law of tort and contract to protect against this result.

66. *See id.* at 660.

67. *Id.* at 667-69.

68. O’Donnell, *supra* note 1, at 679.

69. *See id.*; Randi M. Rothberg, *Not as Simple as Learning the ABC’s: A Comment on Owasso Independent School District No. 1-011 v. Falvo and the State of the Family Educational Rights and Privacy Act*, 9 CARDOZO WOMEN’S L.J. 27 (2002); Daniel R. Dinger, *Johnny Saw My Test Score, So I’m Suing My Teacher*, *Falvo v. Owasso School District, Peer Grading, and a Student’s Right to Privacy Under the Family Education Rights and Privacy Act*, 30 J.L. & EDUC. 575 (2001).

IV. PROTECTION OF APPLICATION FILE INFORMATION

Society holds an indistinct normative perception that personal information should be protectable, at least some of the time. This is reflected in the motley patchwork of legislated privacy regulation,⁷⁰ and

70. See, e.g., Tindall, *supra* note 8, at 190-91; Samuelson, *supra* note 8, at 1144-45; Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 971-72 (a “panoply of federal and state statutes.” See generally Tindall, *supra* note 8, at 181 n.60; Bergelson, *supra* note 8, at 391 (citing the piecemeal implementation of regulations). The legislation includes: Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2000); Children’s Online Privacy Protection Act of 1998, 15 U.S.C. § 6502 (2000); Children’s Internet Protection Act of 2000, 20 U.S.C. § 7001 (2000); Communications Act of 1934, 47 U.S.C. § 222 (2000), amended by Telecommunications Act of 1996, 47 U.S.C. § 222 (2002); Comprehensive Crime Control Act of 1984, 18 U.S.C. § 3141 (2000); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000); Department of Transportation and Related Agencies Appropriations Act of 2002 § 311(a), 115 Stat. 833 (2001) (requiring that “no recipient of funds made available in this Act shall disseminate personal information obtained by a State department of motor vehicles in connection with a motor vehicle record”); Driver’s Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2000); Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522, 2701-2711 (2000); Electronic Funds Transfer Act of 1978, 15 U.S.C. § 1693 (2000); Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (2000); Fair Credit Billing Act, 15 U.S.C. § 1666 (2000); Fair Debt Collections Practices Act, 15 U.S.C. § 1692 (2000); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2000); Financial Services Modernization (Gramm-Leach-Bliley) Act of 1999, 15 U.S.C. § 6801 (2000); Freedom of Information Act, 5 U.S.C. § 552 (2000); Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d (2000); Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028 (2000); Privacy Act of 1974, 5 U.S.C. § 552(a) (2000); Privacy Protection Act, 42 U.S.C. § 2000aa(a) (2000); Right to Financial Privacy Act of 1976, 12 U.S.C. § 3401 (2002) (recognizing individual’s right to privacy with regard to disclosure of financial records by banks to governmental agencies); Telecommunications Act of 1996, 47 U.S.C. § 251 (2003) (offering limited protection to customers’ proprietary information); Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2003) (protecting individuals’ privacy against unwanted phone solicitation); Right to Financial Privacy Act, 12 U.S.C. § 3401 (2000) (providing procedural requirements for sharing financial information among federal agencies); Telemarketing and Consumer Fraud and Abuse Prevention Act of 1991, 15 U.S.C. § 6101 (2000); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2000); CAL. VEH. CODE § 1808.45 (2001) (stating that a right to privacy protects personal information given by individuals to Department of Motor Vehicles); GA. CODE ANN. 40-3-23(e) (2004) (“Personal information of any registrant, including name, address, date of birth, or driver’s license or social security number, shall not be furnished or transferred by or to any person . . .”); MASS. GEN. LAWS. ANN. ch. 66A, § 2(c) (2002) (forbidding “any other agency or individual not employed by the holder [from having] access to personal data” unless it is for purposes of medical treatment, application to professional licenses, special investigation bureau, or for detection of fraud and control); MO. REV. STAT. § 32.091(2) (2001) (prohibiting Department of Revenue from disclosing personal information collected “without express consent given by the person to whom such information pertains”); MONT. CODE ANN. § 61-3-101(8) (2003) (prohibiting Montana Department of Motor Vehicles from furnishing personal information for public inspection); S.C. CODE ANN. § 30-15-60 (Law. Co-op. 1991) (amending South Carolina law to prohibit dissemination of veterans’ discharge records for commercial uses). Cf. Randy Cohen, *The Ethicist, Dead to Rights?*, N.Y. TIMES MAG. Sept. 5, 2004, at 20 (reporting that a young woman feels it would “cause trouble” for her to report adverse information confided to her by a teenager). The author’s view is that such information should be reported if it would prevent injury. See *id.* In this example, a perceived norm of privacy conflicts with the efficient common-law rule against privacy in personal information.

in many polls and surveys. Professor Paul Schwartz, relying on a Harris Equifax poll of public understanding of data protection, observes that a strong majority of those polled felt that “individuals have lost control . . . of personal information.”⁷¹ According to Professor Schwartz, “most individuals believe that they deserve fair information practices that structure the terms by which others . . . gain access” to personal information willingly disclosed.⁷² These observations describe majoritarian expectations reflecting a notion of exchange.⁷³ “Fair information practices” informing a Department of Health, Education and Welfare 1973 report on automated retention of personal information⁷⁴ and international privacy laws similarly include employment of personal information in ways limited to fulfillment of the purposes for which the information was collected and reasonable security safeguards.⁷⁵

This may be especially true in circumstances such as application files, where social institutions require the revelation of important personal information in a highly adhesive relationship established for reasons of high social value. In light of this perceived (albeit indistinct) norm, does the common law protect application file content? This Part

71. Schwartz, *Personal Health Care*, *supra* note 2, at 42. Professor Bergelson cites a poll in which participants “ranked privacy just behind the freedom of speech and ahead of the freedom of religion and the right to vote as the most important American right.” Bergelson, *supra* note 8, at 427 n.255. Bergelson provides a list of other polls which reach similar conclusions. *See id.* at 428 n.260 (citing an EPIC public opinion poll on privacy, an article by Humphrey Taylor, an article by Marlon Manuel, and an IBM-Harris multi-national consumer privacy survey). *See also* Mike Hatch, *The Privatization of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century*, 27 WM. MITCHELL L. REV. 1457, 1476-81 (2001) (listing polls and surveys); Sovern, *supra* note 61, at 1057 (listing polls and surveys).

72. Schwartz, *Personal Health Care*, *supra* note 2, at 44.

73. *Accord* Murphy, *supra* note 3, at 2416 (“[P]rivacy rules are in fact implied contractual terms.”). Professor Jessica Litman has described an indistinct norm of privacy in terms of individuals’ expectations and public adverse response to revelations of certain commercial programs of collection and resale of private facts. *See* Litman, *supra* note 8, at 1304-11. Litman, emphasizing individuals’ foreseeable expectations of the secondary employment of disclosed private facts, suggests a breach-of-trust approach growing out of the norm. *See id.*; *see also supra* notes 27-28 and accompanying text.

74. DEP’T OF HEALTH, EDUC. AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY’S ADVISORY COMMITTEE ON PERSONAL RECORD DATA SYSTEMS (1973), available at <http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm> [hereinafter HEW report]. The HEW Report recommends a Code of Fair Information Practice based on “five basic principles”: There should be no secret systems for keeping personal information records; an individual must be able to know what’s in their file and how it’s being used; an individual must be able to prevent secondary employment of their personal information; an individual must be able to correct erroneous personal information; and an information-collecting organization must assure reliability of data for intended uses and take precautions to prevent misuse. *Id.* at 1. The Summary and Recommendations section of the report characterizes information collection as “trading” and concludes that “both parties to the exchange should participate in setting the terms.” *Id.*

75. *See* Gellman, *supra* note 43, at 5-6.

reviews the limited ways in which the common law protects personal information. It will show that the protective nexus is not a norm of privacy but rather a focus on how personal information comes into the hands of parties other than the subject, and on what use is made of it afterward. Privacy, in the sense of being “let alone,”⁷⁶ or keeping secrets, or the subject’s control of secondary employment, is not the informing value of such regulation as there is; rather, the informing value is the wrongfulness under other norms⁷⁷ of either the act of obtaining personal information or of re-employing it. As will be seen, the present state of common-law regulation offers little protection to application-file content.

A. *Protection of Private Facts: The Common Law*

Given that the common law allocates the risk of excessive secondary employment to the applicant, does the common law protect application-file information? Ownership of information is regulated by the courts through the common law, and the application of *stare decisis* normalizes judge-made regulation. The common law has largely disfavored a right of privacy in truthful, legally obtained personal information⁷⁸ outside of relationships of trust and confidence.⁷⁹ In particular, it gives little protection to private facts.⁸⁰

In terms of secondary employment by schools, common-law protection is very slight. Under the common-law default rule of disclosure, speaking generally, “facts about people” are not protected.⁸¹ The manner of obtaining facts about people is regulated, but only to the extent that it inflicts cost by altering the subject’s behavior.⁸² Secrets

76. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

77. See Bergelson, *supra* note 8, at 394 (courts have “refused to recognize the plaintiffs’ [privacy] claims since they did not fit under the existing categories of protected interests”); see also *infra* notes 111-112 and accompanying text.

78. See Posner, *Right of Privacy*, *supra* note 20, at 399.

79. See, e.g., *Vassiliades v. Garfinckel’s*, 492 A.2d 580, 591 (D.C. 1985) (quoting authority for the proposition that the relationship supporting a tort of breach of confidence is one customarily including a duty of confidence); see also W. PAGE KEETON ET AL., PROSSER AND KEATON ON TORTS 121 (5th ed. 1984). Cf. MODEL CODE OF PROF’L RESPONSIBILITY Canon 4 (1999); MODEL CODE OF PROF’L RESPONSIBILITY R. 1.6 (1999).

80. See, e.g., Litman *supra* note 8, at 1304 (concluding that “the invasion of privacy tort is too narrowly defined to serve” as a “solution to the problem of personal data privacy”); *id.* at 1311 (“Current tort law does not offer much protection for an individual’s data privacy.”).

81. Posner, *Right of Privacy*, *supra* note 20, at 404.

82. See *id.* The use of “intrusive surveillance” to obtain facts about people is appropriate only to law enforcement, according to Judge Posner. See *id.*; see also *infra* notes 104-108 and accompanying text (demonstrating limits on even First Amendment-protected newsgathering).

representing the application of superior knowledge or skills are protected against revelations that might discourage socially valuable conduct, a general result permitting commercial enterprises to keep secrets for commercial advantage.⁸³ These general results are described by Judge Posner as the parameters of a “legal right of privacy based on economic efficiency,”⁸⁴ an economics-informed norm. The common law protection of information conveyed in the context of a relationship of trust and confidence, while extended to students,⁸⁵ has not been extended to the applicant/school relationship.⁸⁶

Modern analysis of common-law privacy rights in this country famously began with *The Right to Privacy*, the Warren and Brandeis article published in 1890.⁸⁷ The article articulates a broad norm of privacy, affirming in personal information a “right of property in its widest sense,” with remedies in tort.⁸⁸ Warren and Brandeis’ powerful normative argument found wide scholarly acceptance⁸⁹ and a place in the first Restatement of Torts.⁹⁰ Attempts to apply their argument experienced rough sledding in the courts, however. The narrowness of the degree of acceptance of privacy as a protectable interest was delineated by Dean William Prosser in his 1960 exegesis of the cases.⁹¹ Dean Prosser sorted the cases into the four now-familiar categories of intrusion of an unreasonable and offensive nature,⁹² public disclosure of

83. See Posner, *Right of Privacy*, *supra* note 20, at 404.

84. *Id.*

85. See, e.g., *Bridges v. MacLean-Stevens Studios, Inc.*, 201 F.3d 6, 11 (1st Cir. 2000) (“Unquestionably, the schools and the students enjoy a special relationship of trust.”) (quoting *Stephen Jay Photography, Ltd. v. Olan Mills, Inc.*, 903 F.2d 988, 993 (4th Cir. 1990)).

86. See, e.g., Ian Goldberg et al., *Trust, Ethics, and Privacy*, 81 B.U. L. REV. 407 (2001); Helen Nissenbaum, *Securing Trust Online: Wisdom or Oxymoron?*, 81 B.U. L. REV. 635 (2001); see also Litman, *supra* note 8, at 1284-86, 1304-11.

87. Warren & Brandeis, *supra* note 76.

88. *Id.* at 210-11. Property rights continue to be put forward as a vehicle for protection of private facts. See e.g., Bergelson, *supra* note 8; Schwartz, *Property*, *supra* note 5; George P. Smith, II, *The Extent of Protection of the Individual’s Personality Against Commercial Use: Toward a New Property Right*, 54 S.C. L. REV. 1 (2002); Sovern, *supra* note 61. The movement to protect privacy through property rights has achieved little success in the courts. See Litman, *supra* note 8.

89. See, e.g., KEETON ET AL., *supra* note 79, at 850 (following publication of the Warren and Brandeis article, “no other tort has received such an outpouring of comment in advocacy of its bare existence.”).

90. RESTATEMENT (FIRST) OF TORTS § 867 (1939).

91. See William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960); see generally KEETON ET AL., *supra* note 79, at 849-69.

92. This tort relates to methods of obtaining information that “would be offensive or objectionable to a reasonable person.” KEETON ET AL., *supra* note 79, at 855. Judge Posner describes it as “obtaining of personal information by intrusive means,” and gives as examples interfering with a person’s “movements” and eavesdropping. Posner, *Economics of Privacy*, *supra* note 58, at 408.

embarrassing private facts, publicity placing the subject in a “false light,”⁹³ and appropriation, for financial gain, of a subject’s name or likeness.⁹⁴ These categories, accepted in the Second Restatement⁹⁵ (hereinafter “Restatement”), furnish the present common-law analytical framework of a protectable interest in privacy.

Of the Restatement’s four categories, two are of manifest significance to the present topic: intrusion⁹⁶ and private facts.⁹⁷ Private facts will be discussed first.

1. The Restatement Private Facts Tort

Private facts have received little common-law protection.⁹⁸ Three main themes run through the literature describing the failure of the private-facts tort to achieve broad acceptance: The tort’s inconsistency with constitutionally protected rights of speech and publication, its ambiguity in terms of what constitutes a protectable interest, and economic inefficiency. These threads are woven against a background of privacy interests so widely various as to defeat any clear articulation of a unifying theme of protectability.

Once acquired by a person other than the subject, personal information can be re-employed in multiple ways, including as gossip, as data informing such criminal acts as identity theft, as lawfully acquired tidbits that, in the aggregate, can create value (magazine publishers aggregating and selling subscription lists, for example), as subject matter to attract buyers to the popular press, and in numberless other ways in which value (either financial or in the form of personal satisfaction) can accrue to a new possessor and cost (ranging from a mere personal preference for privacy to identity theft) to the subject. These extremely varied interests and conflicting claims on the value inherent in private

93. This tort is said to protect against knowingly false publications of a nature “highly offensive” to a reasonable person. See KEETON ET AL., *supra* note 79, at 865.

94. This tort is oriented toward preventing another from benefiting economically from the use of a subject’s name or likeness without permission; the cases relate to uses in advertising. See Posner, *Economics of Privacy*, *supra* note 58, at 408.

95. RESTATEMENT (SECOND) OF TORTS § 652A (1977).

96. “One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.” *Id.* at § 652B.

97. “One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.” *Id.* at § 652D.

98. See Posner, *Economics of Privacy*, *supra* note 58, at 408 (“Examination of the cases shows . . . that the right is upheld in very few cases.”); G. Michael Harvey, Comment, *Confidentiality: A Measured Response to the Failure of Privacy*, 140 U. PA. L. REV. 2385, 2403-21 (1992).

facts seem to have precluded articulation of a unifying normative theme.

The Restatement formulation as employed in the courts describes the “private facts” tort as limited to facts which, while truthful, are ones as to which “publicity” would be “highly offensive to a reasonable person.”⁹⁹

As to its “publicity” prong, the private-facts tort described in the Restatement does not relate to how private facts are obtained—that is confined to the “intrusion” tort, discussed next—but to re-disclosure, or secondary employment. Lawfully obtained private facts are protected from only a single manner of re-disclosure, “giv[ing] publicity,” in the Restatement’s words.¹⁰⁰ The Restatement’s definition of publicity is communication to the “public at large” or re-employment in such a way as to be “substantially certain to become . . . public knowledge,”¹⁰¹ which, in a practical sense, is most likely to apply to repetition by the news media. Attempts to prove in court a tort so delineated have largely failed.¹⁰² This failure is attributable in part to conflict with constitutionally protected speech: According to Justice White, Supreme Court speech-rights analysis has “obliterate[d]” the possibility of protecting private facts from publication in the Restatement sense, so long as the information is lawfully obtained.¹⁰³ It is further attributable to ambiguity.¹⁰⁴ Even if these obstacles are overcome, no action lies if the matter publicized is “of legitimate public concern,”¹⁰⁵ that is,

99. RESTATEMENT (SECOND) OF TORTS § 652D cmt. c (“It is only when the publicity . . . is such that a reasonable person would feel justified in feeling seriously aggrieved by it, that the cause of action arises.”).

100. The word “publicity” is used both in the title section, “Publicity Given to Private Life,” and in the text. *Id.* at § 652D cmt. a.

101. *Id.*

102. See, e.g., Jonathan B. Mintz, *The Remains of Privacy’s Disclosure Tort: An Exploration of the Private Domain*, 55 MD. L. REV. 425 (1996); Bergelman, *supra* note 8, at 394-400.

103. *Florida Star v. B.J.F.*, 491 U.S. 524, 550 (1989) (White, J., dissenting).

104. By far, most reported cases (and therefore much of the law) involving attempts to protect personal information involve publication of such information in a manner implicating the First Amendment. See, e.g., Eric W. Tiritilli, *You Never Call Me Anymore: Bartnicki v. Vopper and the Supreme Court’s Abridgement of the Right of Privacy in Favor of the First Amendment Right of a Free Press*, 35 CREIGHTON L. REV. 729 (2003); Mintz, *supra* note 102; Sean M. Scott, *The Hidden First Amendment Values of Privacy*, 71 WASH. L. REV. 683 (1996); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1117 (2000); Harvey, *supra* note 98, at 2401-22 (describing “the death of the private facts tort”). In the few cases reaching the United States Supreme Court, constitutionally protected speech has always outweighed a personal interest in privacy. See generally *Bartnicki v. Vopper*, 532 U.S. 514 (2001); *Florida Star*, 491 U.S. 524; *Smith v. Daily Mail Publ’g Co.*, 443 U.S. 97 (1979); *Okla. Publ’g Co. v. Dist. Court*, 430 U.S. 308 (1977); *Cox Broad. Corp. v. Cohn*, 420 U.S. 469 (1975).

105. RESTATEMENT (SECOND) OF TORTS § 652D cmt. d. Warren and Brandeis themselves carve out from protection the “publication” of facts “of public or general interest.” Warren &

“newsworthy,” as the literature has it.

The Restatement, by its terms, does not describe a tort protective of private facts based on “publication” in the sense of simple repetition, as distinguished from “publicity.”¹⁰⁶ A few cases recognize such a tort by bending the Restatement’s limitation to publicity “to the public at large,”¹⁰⁷ but these few cases lean strongly on a perceived norm of outrage in particular cases. Any more-general recognition has been defeated by the aforementioned obstacles of subjectivity of valuation, and ambiguity.¹⁰⁸ This is probably as the Restatement intends.

Some cases take the view that willing disclosure of information by the subject to another, or to a small group, does not necessarily mean that private facts cease being private.¹⁰⁹ Most such cases contain strong elements of contract or confidential relationships, however.¹¹⁰ They also manifest elements of subjective, rather than objective, outrage, demonstrated by the plaintiff’s suffering.¹¹¹

Private facts in this sense are protected not as property—as Warren and Brandeis would have it—but according to a vague norm of offensiveness, tested objectively, the “highly offensive” prong of the Restatement description. The Restatement illuminates this norm using terms including “highly offensive to the ordinary reasonable man,”¹¹² “mores of the community,”¹¹³ and “common decency.”¹¹⁴ These terms

Brandeis, *supra* note 76, at 214.

106. See RESTATEMENT (SECOND) OF TORTS § 652D cmt. a; see also DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 90 (1972).

107. KEETON ET AL., *supra* note 79, at 856-57.

108. See Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis’s Private Tort*, 68 CORNELL L. REV. 291, 337 (1983) (courts avoid the “legal tangle” of subjecting “gossip to liability”); see also Steven I. Katz, Comment, *Unauthorized Biographies and Other “Books of Revelations”: A Celebrity’s Legal Recourse to a Truthful Public Disclosure*, 36 UCLA L. REV. 815, 816 (1989) (gossip among individuals “cannot practically speaking be the basis of a cause of action . . .”).

109. See, e.g., *Virgil v. Time, Inc.*, 527 F.2d 1122, 1127 (9th Cir. 1975) (disclosure to a reporter of private facts for which consent to republication was expressly withdrawn does not render the facts public); *Times Mirror Co. v. Superior Court*, 244 Cal. Rptr. 556, 561 (Cal. Ct. App. 1988) (subject disclosing personal information in connection with a criminal investigation does not thereby render the information public). Cf. *Miller v. Motorola, Inc.*, 560 N.E.2d 900, 903 (Ill. App. Ct. 1990) (“publicity” does not require general publication; publication of fact of mastectomy to fellow employees was sufficient).

110. Cf. *Virgil*, 527 F.2d at 1127 (consent to republish withdrawn); *Miller*, 560 N.E.2d at 902 (breach of understanding of confidence by employer’s staff nurse).

111. See, e.g., *Miller*, 560 N.E.2d at 902 (plaintiff whose mastectomy was disclosed to co-workers alleged “severe physical, mental and emotional distress” and took early retirement).

112. RESTATEMENT (SECOND) OF TORTS § 652D cmt. c.

113. *Id.* at § 652D cmt. g.

114. *Id.* at § 652D cmt. h.

have been criticized as “so conceptually vague that they offer little guidance,”¹¹⁵ and as being “hopelessly ambiguous.”¹¹⁶

Clearly, the private-facts tort in the common law does not protect application file information except in the most narrow of circumstances. Certainly it does not provide any deterrent or remedy that would be generally applicable.¹¹⁷

2. The Restatement Intrusion Tort

The intrusion tort is not designed to control content, but the manner in which information is acquired. Under the Restatement version, one who obtains private facts “intrusively” within the meaning of the tort has committed a wrong even if the information is never re-disclosed.¹¹⁸ “Intrusion” requires that two elements be shown: Intrusion upon the “solitude or seclusion of another or his private affairs,” in a manner “highly offensive to a reasonable person,”¹¹⁹ an objective standard. Other renditions of the tort differ slightly.¹²⁰ Generally speaking, information voluntarily surrendered fails the “intrusion” prong, and widely available information fails the “highly offensive” prong.¹²¹

Whether a particular example of information gathering constitutes intrusion is highly problematic.¹²² Compare, for example, the Ninth Circuit’s opinion in *Dietemann v. Time, Inc.*,¹²³ with Judge Posner’s Seventh Circuit’s opinion in *Desnick v. American Broadcasting Cos.*,

115. Zimmerman, *supra* note 108, at 301.

116. Randall P. Bezanson, *The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1900*, 80 CAL. L. REV. 1133, 1171 (1992).

117. See Bergelson, *supra* note 8, at 408 (requirement of publication “more or less disqualifies this tort as a possible cause of action for plaintiffs attempting to control the use and transfer of their personal information”).

118. RESTATEMENT (SECOND) OF TORTS § 652B cmts. a-b.

119. *Id.* at § 652B.

120. See, e.g., Bergelson, *supra* note 8, at 406 (citing authority for a four-element test: “(i) an unauthorized intrusion or prying into the plaintiff’s seclusion; (ii) which is offensive or objectionable to a reasonable person; (iii) as to a matter which is private; and (iv) which has caused anguish and suffering”); Scott Shorr, Note, *Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment*, 80 CORNELL L. REV. 1756, 1778 (1995) (describing a three-part test: “the intrusion must (1) be highly offensive to a reasonable person; (2) be intentional; and (3) occur in a place where the plaintiff has a reasonable expectation of privacy”).

121. See Shorr, *supra* note 120, at 1778-79.

122. In the news-gathering context, the act of gathering is not as strongly constitutionally protected as is publication. “Newsworthiness” is a “complete bar to liability for publication of private facts,” but the news gatherer’s “right to intrude” receives much more limited protection. Only depriving news gatherers of “indispensable tools” is protected. *Shulman v. Group W Prods., Inc.*, 955 P.2d 469, 496 (Cal. 1998) (citing *Dietemann v. Time, Inc.*, 449 F.2d 245, 249 (9th Cir. 1971)).

123. 449 F.2d 245 (9th Cir. 1971).

*Inc.*¹²⁴ Both cases involve news-gatherers visiting the plaintiffs' premises under false pretenses and surreptitiously obtaining tapes and photos. In *Dietemann* the Ninth Circuit had "little difficulty" in deciding that the reporters' actions "warrant[ed] recovery for invasion of privacy in California."¹²⁵ In *Desnick*, by contrast, Judge Posner, writing for the court, found no intrusion upon seclusion. The difference, he explained, was that the reporters in *Dietemann* entered the plaintiff's home on a purported social visit, while in *Desnick* the reporters entered the plaintiff's place of business for the purported purpose of a medical examination. According to Judge Posner, in *Desnick* there was "no invasion . . . of any of the specific interests that the tort of trespass seeks to protect . . . nor was there any 'inva[sion of] a person's private space.'"¹²⁶ Notably, Judge Posner's analysis of "intrusion" was strongly linked to a norm of trespass.

Analytically the intrusion cases rely heavily on reasonable expectations and the closely related notion of "custom."¹²⁷ Courts have protected privacy expectations in houses and ambulances.¹²⁸ In *Desnick* the space held not to be protected was the plaintiff's place of business, where customarily, the public was invited.¹²⁹

It has been held that "seclusion" does not mean absolute seclusion.¹³⁰ Indeed, "[t]he mere fact that a person can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone."¹³¹

The second prong of the Restatement intrusion tort is that the intrusion must be "highly offensive" in an objective sense.¹³² The cases do not draw a strong distinction between what's intrusive and what's

124. 44 F.3d 1345 (7th Cir. 1995).

125. *Dietemann*, 449 F.2d at 248.

126. *Desnick*, 44 F.3d at 1352 (citing *DeMay v. Roberts*, 9 N.W. 146, 146, 149 (Mich. 1881) (physician held liable when he brought a non-physician friend along to a patient's home to witness a birth)).

127. See, e.g., *Shulman v. Group W Prods., Inc.*, 955 P.2d 469, 490, 491 (Cal. 1998) ("[W]e are aware of no law or custom permitting the press to ride in ambulances or enter hospital rooms during treatment without the patient's consent." The plaintiff could "reasonably have expected" conversations in the ambulance to be private.); *Dietemann*, 449 F.2d at 249 ("Plaintiff's den was a sphere from which he could reasonably expect to exclude eavesdropping newsmen.").

128. See *supra* note 127 and accompanying text.

129. See *Desnick*, 44 F.3d at 1352.

130. See, e.g., *Bergelson*, *supra* note 8, at 406 ("The intrusion does not have to be of a physically defined place.").

131. *Sanders v. Am. Broad. Cos., Inc.* 978 P.2d 67, 72 (Cal. 1999) (quoting 1 J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 5.10[A][2], 5-120.1 (1998), as adopted by *Shulman*, 955 P.2d at 490 (holding that surreptitiously taping the plaintiff's conversations with co-workers violated the plaintiff's right of seclusion)).

132. RESTATEMENT (SECOND) OF TORTS § 652B.

highly offensive. Once intrusion is found, high outrage seems to follow. In *Shulman v. Group W Productions, Inc.*,¹³³ for example, the court (in a summary judgment context) held that a newsperson's entry into an air ambulance was intrusion (based on a reasonable expectation of privacy) and that taping and filming the plaintiff was sufficient that "a jury could find . . . filming in the air ambulance, to be 'highly offensive to a reasonable person'" and to show "highly offensive disrespect for the patient's personal privacy."¹³⁴

Is access to application files intrusion? In the higher education context, intrusion is not relevant to primary disclosure of application-file information, because it is willing as to the subject. It is probably not relevant even to secondary disclosure by the schools, for failure of the intrusion prong.¹³⁵ In at least one case, a clear example of excessive secondary employment, disclosure of personal medical information was held to be an "invasion of privacy."¹³⁶ The analysis is akin, however, to protection within a relationship of trust and confidence—again, the content of the wrong being a link to an existing norm, not a norm of privacy.

Where intrusion may be relevant in the admissions context is in the access to files by persons from whom the applicant has a reasonable expectation of privacy. These would almost certainly be intruders not part of the university community. As I understand the current regime, the applicant has little expectation of privacy with respect either to disclosure (file access) to university staff or to purposeful secondary employment. Intrusion has been significantly limited in the cases in ways that reduce its deterrent function in the context of application files. The New York Court of Appeals, for example, has held that "there can be no invasion of privacy where the information sought . . . has been

133. 955 P.2d 469 (Cal. 1998).

134. *Id.* at 494-95.

135. *Cf. Reno v. Condon*, 528 U.S. 141, 144-51 (2000) (holding valid the amended Driver's Privacy Protection Act of 1994, allowing for secondary disclosure when a driver "opts-in" to such disclosure); *Kehoe v. Fid. Fed. Bank & Trust*, No. 04-13306, 2005 U.S. App. LEXIS 18406, at *1-23 (11th Cir. Aug. 26, 2005); *In re Charter Commc'ns, Inc.*, 393 F.3d 771, 784-85 (8th Cir. 2005) (holding compliance with subpoenas issued under Digital Millennium Copyright Act paramount to consent to disclosure of information); *Schuchart v. La Taberna del Alabardero, Inc.*, 365 F.3d 33, 36 (D.C. Cir. 2004) (recognizing that some states find liability when disclosure exceeds scope of consent); *In re Pharmatrak, Inc.*, 329 F.3d 9, 19 (1st Cir. 2003) (interpreting a statutory consent exception to disclosure protection under the Electronic Communications Privacy Act as contingent on the scope of the consent given by the subject).

136. *See, e.g., Commonwealth v. Brandwein*, 760 N.E.2d 724, 729 (Mass. 2002) (recognizing that "disclosure of confidential medical information . . . can constitute an actionable tort, or an invasion of privacy"); Alan B. Vickery, Note, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426, 1441 (1982); Judy E. Zelin, Annotation, *Physician's Tort Liability for Unauthorized Disclosure of Confidential Information About Patient*, 48 A.L.R. 4th 668, 680 (1986).

voluntarily revealed to others.”¹³⁷ Intrusion has also been held not to lie as to those who secondarily obtained and made use of information obtained by others.¹³⁸

In short, applicant-file information is not meaningfully protected by the common-law privacy torts. The subject matter of the recognized torts is too limited, and even they provide almost no *ex ante* deterrence or *ex post* compensation.¹³⁹ As Professor Schwartz observes, in some instances “litigation for privacy violations under a tort theory has foundered because courts determined that the actual harm that the plaintiffs suffered was *de minimis*.”¹⁴⁰ He further observes that personal information “may not have a high enough market value to justify the costs of litigation.”¹⁴¹ This won’t be true in all cases, of course—consider the “market value” of identity theft—but it may well be the case in a sufficient preponderance of cases to prevent development of a viably protective tort remedy with its inevitable cost effects.

Finally, so long as schools preserve their adhesive, asymmetrical grip on information about secondary employment, it is simply unlikely that applicants will discover these uses and be able to prove the requisites of the Restatement privacy torts.¹⁴² As one observer has put it, “the privacy tort seems structurally incapable of securing . . . control over personal information.”¹⁴³

B. *Protection of Private Facts: Contract*

While it has been argued that contract could provide a basis for protecting private facts,¹⁴⁴ in the present admissions regime contract does not provide a satisfactory basis. One reason is that applicants are “privacy myopic”—they are not aware of the market value of their personal information and therefore are not aware of the risk of its

137. *Nader v. Gen. Motors Corp.*, 255 N.E.2d 765, 769 (N.Y. 1970) The court held that “[i]nformation about the plaintiff which was already known to others could hardly be regarded as private” and that the plaintiff would “necessarily assume the risk” of re-publication. *Id.* at 770. *Accord* *Dwyer v. Am. Express Co.*, 652 N.E.2d 1351, 1354 (Ill. App. Ct. 1995) (use of plaintiff cardholder’s personal information revealed by use of the card is not intrusion). *But see Sanders*, 978 P.2d at 69 (a reporter’s surreptitious taping of plaintiff’s conversations with co-workers intruded upon plaintiff’s seclusion).

138. *See Pearson v. Dodd*, 410 F.2d 701, 705-06 (D.C. Cir. 1969) (noting that newspaper writers who accepted and used copies of documents they knew had been wrongfully obtained not liable for invasion of privacy).

139. *See Tindall*, *supra* note 8, at 191.

140. Schwartz, *Property*, *supra* note 5, at 2108.

141. *Id.*

142. *Cf. Shorr*, *supra* note 120, at 1791-92.

143. *Id.* at 1794.

144. *See, e.g., id.* at 1834-50.

secondary employment. Meaningful bargaining is obviated by information cost. The other is that, even if meaningful bargaining were available, transaction cost would degrade the efficiency of the present admissions regime. These two points are discussed in order below.

1. The Failure of Accurate Valuation: “Privacy Myopia”

Consumers generally are said to be “privacy myopic.”¹⁴⁵ Professor Froomkin employs this term to describe consumers’ persistence in undervaluing personal information, valuing it at its marginal value to themselves rather than at its (higher) value in the marketplace for personal information.¹⁴⁶ Such undervaluation results in over-disclosure by subjects,¹⁴⁷ assuring a market among those seeking to capture the valuation differential. As a result, consumers part with personal information “too often and too cheaply.”¹⁴⁸ This is related to the well-documented tendency of individuals to underinsure low-probability, high-risk future events.¹⁴⁹

As noted elsewhere in this Article,¹⁵⁰ society holds an indistinct notion valuing privacy, an indistinct norm based on a privacy preference. Privacy myopia demonstrates that individuals’ actions do not comport with the norm.¹⁵¹ Studies show that consumers part with personal information often and cheaply even when they claim to value privacy.¹⁵² Thus, “privacy myopic” has been used to describe a person who, “even if she professes to appreciate privacy, does not take actions to protect herself”¹⁵³

Failure of a person professing a privacy preference to self-protect—parting with personal information too often and too cheaply—may be based on a number of factors relevant in the present context, including

145. Froomkin, *supra* note 2, at 1502.

146. *Id.* at 1503. *See also* Acquisti & Grossklags, *supra* note 55, at 3 (“[E]ven privacy concerned individuals are willing to trade-off privacy for convenience or to bargain the release of very personal information in exchange of relatively small rewards.”).

147. Froomkin, *supra* note 2, at 1504.

148. *Id.* at 1502. *Accord* Acquisti & Grossklags, *supra* note 55, at 3 (citing studies showing that “even privacy concerned individuals are willing to trade-off privacy for convenience or to bargain the release of very personal information in exchange of relatively small rewards”); Tindall, *supra* note 8, at 187 (“Consumers appear to be perfectly willing to offer businesses a startling amount of private information.”).

149. *See* Acquisti & Grossklags, *supra* note 55, at 11.

150. *See* Murphy, *supra* note 3.

151. *See, e.g.*, Karas, *supra* note 4, at 420, 421 (“Although consumers tend to voice concerns about privacy, they routinely part with personal data . . . [they] simply tend to value the convenience of online shopping and marginal financial gain over the potential privacy threats of data collection.”).

152. *See, e.g.*, Sovern, *supra* note 61, at 1067-94.

153. *See* Acquisti & Grossklags, *supra* note 55, at 12.

lack or asymmetry of information, bounded rationality (“rational ignorance”), and market behavior focused on “short-term factors.”¹⁵⁴

Incomplete information is clearly a factor influencing disclosure in the admissions context. Applicants do not know everything that’s in their files. It is worth remembering in this respect that applicants don’t provide all of the information in their files. Instead, they permit a collection of information about themselves to be compiled from a variety of sources. Applicants cannot assess the value of the collection accurately because they do not know all that’s in it, and with respect to some items they are aware of, such as letters of recommendation, they are prevented from learning the content.

Even if applicants did know of everything in their files, they would not know how to value it because they cannot predict risk.¹⁵⁵ They don’t know what a particular school’s file security is like or what its intentions are relative to secondary employment. In short, applicants are dramatically subject to information asymmetry.¹⁵⁶ The present application process cannot be analyzed in terms of a fully rational model.

Accordingly, applicants cannot accurately assess disclosure risk. For this reason if no other, self-protection through bargaining is unavailable.

Further, in the highly adhesive context of admissions, the possibility of negotiating with schools over disclosure likely never occurs to applicants. In a sense, a transaction is taking place in which one party, the applicants, are not aware that bargaining is a possibility, much less that the information they supply might be further employed.¹⁵⁷

Closely related to information asymmetry are the effects of bounded rationality. The unpredictability of the complex effects, and costs, of unanticipated secondary employment of personal information defeats cost-benefit assessment. The cost of protection, including prediction, calculation, and negotiation might well be perceived by applicants as higher than the foreseeable cost of loss of privacy. Accordingly, applicants do not make the attempt.¹⁵⁸ The valuation process itself is costly, and indeed I would suggest prohibitively costly

154. *Id.*

155. *See, e.g.,* Samuelson, *supra* note 8, at 1145 (observing difficulty of “the average person to judge the risks of selling her property rights in personal data”).

156. *See* Schwartz, *Property*, *supra* note 5, at 2081 (describing information asymmetry as a problem in privacy markets).

157. *Cf. id.* at 2078 (characterizing such a situation as an “extreme illustration of privacy market failure”).

158. Acquisti & Grossklags, *supra* note 55, at 9-10. Professor Schwartz characterizes this as a consumer’s “general inertia toward default terms.” Schwartz, *Property*, *supra* note 5, at 2081.

in light of all the possibilities that must be taken into account, so that privacy myopia may in fact largely consist of short-term cost avoidance.

Applicants' unlikely of incurring the cost of risk assessment seems particularly likely should applicants take a short-term view of risk. Market behaviors focusing on the short term may result in acts inconsistent with professed privacy preferences. A short-term focus can overcome a perception that risk is high but long-term and low-probability.¹⁵⁹ In the case of applicants, the opportunity to enter the admissions market might well represent a well-defined, high value, but short-term benefit that overcomes a more strategic analysis of privacy risk.

In some cases the weighing of secondary-employment cost and the assessment of socially beneficial actions simply do not come into play because the requirement of self-disclosure is so highly adhesive that a subject motivated to apply has no choice. They must accept the school's conditions, or relinquish the opportunity to apply. Again, health care disclosures are an example,¹⁶⁰ and so in many cases are school applications. In this respect, highly adhesive privacy regimes are inherently inefficient.

Of course, even a rational, perfectly informed consumer faced with zero transaction cost will exchange personal information for something they value more highly.¹⁶¹

All of the foregoing factors will contribute to both an inability to bargain and a possible lack of motivation to bargain,¹⁶² reducing the possibility of an applicant self-protecting with respect to application-file information. Again, the transmission of personal information through the admissions process does not operate within a fully rational model. This suggests that market correction is not available.

The magazine-subscription example, accordingly, is probably not applicable to secondary employment of application-file content. The example might suggest that students value their privacy less than the opportunity of being considered for admission. This assumes rational decision-making based on full information, or a correct assessment of very low-value-low-risk information. While this is probably accurate in the context of primary employment, the complex nature of application files, taken together with the prospects of limited and asymmetrical

159. Acquisti & Grossklags, *supra* note 55, at 11.

160. See generally Schwartz, *Personal Health Care*, *supra* note 2.

161. See, e.g., Richard A. Epstein, *Holdouts, Externalities, and the Single Owner: One More Salute to Ronald Coase*, 36 J.L. & ECON. 553, 555 (1993); Sovern, *supra* note 61, at 1083-84.

162. Cf. Samuelson, *supra* note 8, at 1151 ("[M]arket imperfections make it difficult to negotiate effectively about terms of use as to personal data.").

information, bounded rationality, and market behaviors suggest to the contrary in the context of secondary employment. Combined with the high social benefit of the higher-education admissions process, this explains the extravagantly adhesive relationship that is permitted to exist in the admissions process.

So long as individuals undervalue their personal information relative to its market value, there will be a buyer for it in today's information-hungry economy.¹⁶³ Those coming lawfully into possession of personal information about others who have a market basis on which to value such information are the beneficiaries of the default rule of disclosure. Personal information will persist in being undervalued so long as the subject is unaware of the risk of revealing it. In any event, the cost to the individual of accurate valuation will be prohibitively high.

This section has shown that subjects of personal information are not interested in selling it and not equipped or motivated to bargain. They do willingly "sell," in the sense of exchange, certain types of personal information for more highly valued opportunities, such as to apply to universities. Indeed, in exchange for such opportunities they will willingly exchange even very high-value personal information that they would be unlikely simply to sell for cash. Thus the point of regulation of secondary employment of personal information is not how the information gets into other hands in the first place, the point is what happens to it afterward and the subject's difficulties both in assessing risk and in controlling the answer to that question.¹⁶⁴

2. The Admissions Inefficiencies of Negotiation

Negotiated private-law arrangements—contracts—constitute private-law regulation through negotiated allocation of risk and cost. Generally speaking, contract is efficient, employing bargained

163. See, e.g., Froomkin, *supra* note 2, at 1465 (observing that there is enormous and growing demand for personal information).

164. See, e.g., Karas, *supra* note 4, at 409-10. The notion of "privacy" is actually a notion of ability to control "circulation of information relating to oneself." *Id.* (citing ARTHUR R. MILLER, ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 23 (1971); *id.* at 423 ("[T]he core impulse in . . . [trying to regulate] privacy scandals is controlling information, not getting paid for it."). Karas goes on to observe that "privacy should be framed not as mere control over personal information, but rather information that expresses one's identity." *Id.* at 427 (citing Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133, 154-56 (1991); Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 236 (1977)). Unless Karas is suggesting that regulation be based on some sort of paternalistic judgment, he should consider that "privacy," a uniquely personal concept, constitutes a matrix of personal decisions about what to exchange for what, efficiency in an economic sense. Government regulation of personal decisions is like a stopped clock—it gets these kinds of considerations right only occasionally. It's the default rule that's key. It should be reversed.

exchanges to transfer rights in goods and services to persons who value them more highly than do the transferors.¹⁶⁵ Economics assumes that in a contractual exchange each party obtains a good or service that they value more highly than that which they exchanged, a result that is privately and socially efficient. By the same token, a party's refusal to exchange demonstrates that they value what they have more highly than what is being offered in exchange, and that also is efficient.

The perceived private and social benefits of private-law regulation are demonstrated by the insight of Professor Ronald Coase, that where transaction cost is sufficiently low, in rationally seeking to maximize their respective best interests parties to a transaction will bargain away from initial allocations of risk and cost toward mutually satisfactory allocations.¹⁶⁶ Negotiated outcomes will accordingly tend toward private and social efficiency.

"Initial allocations" in this context refers to the starting point for bargains. In patterns of bargaining that feature many similar transactions, efficiency suggests normalized starting places—default rules. These are the common-law starting places for private-law bargains.

Efficiency further suggests that default rules not be random but rather be either majoritarian or coercive, depending on the degree of informational and bargaining symmetry in particular transactions. Where information and bargaining power are reasonably symmetrical, a default rule can appropriately be set as that which would be the result of the majority of negotiations. Such majoritarian default rules reduce transaction cost across the board both by reducing the number of transactions in which the parties would find it necessary to negotiate out of the default rule,¹⁶⁷ and by setting a workable rule to regulate transactions in which the parties do not negotiate the point. In either case, efficiency is enhanced over the long run.

Coercive default rules are set so as to disadvantage a party that would otherwise benefit from an information asymmetry, stimulating such a party to initiate bargaining and reveal such information as the price of negotiating around the rule.¹⁶⁸

As transaction cost (including information cost) rises, initial allocations of risk and cost are correspondingly less likely to be adjusted through bargaining to an efficient result. High transaction cost, and particularly asymmetrical information cost, reduces the efficiencies of

165. See POSNER, *ECONOMIC ANALYSIS*, *supra* note 27, at 93-98.

166. See Ronald H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960).

167. See, e.g., Murphy, *supra* note 3, at 2412.

168. *Id.* at 2413-16.

contract as private regulation because it interferes with the bargain. When transaction cost is high default rules are correspondingly less likely to be negotiated around, so that the default rule tends toward the mandatory, to the advantage of the party benefiting from the default rule. The market becomes less free (and therefore less efficient). Effectively, regulation is performed by the person setting the default rule. It therefore becomes important to know who assigns default rules, and on what basis. In some sectors public institutions assume a regulatory role, creating mandatory rules (ruling out bargaining) or default rules and sometimes a mixture of the two (business corporation statutes, for example). In privately regulated transactions default rules may be set by market norms or may be set inferentially by common-law outcomes. More to the present point, default rules may also be set by oligopolistic possessors of scarce resources in a position persistently to set default rules (for example, cable television companies in consumer transactions)¹⁶⁹ or by a class of contracting parties with characteristically superior knowledge and bargaining leverage over their opposite numbers (think of lawyers, relative to their clients). Because of the unlikelihood of any revision of the default rule in such cases, the resulting transactions will have adhesive qualities. Depending upon the desirability, or the necessity, of access to the goods or services offered by such parties, adhesive qualities give the advantaged party access to opportunistic or rent-seeking behaviors. When default rules are set in this way the result is socially and privately inefficient because they tend to over-compensate the advantaged party.¹⁷⁰

The efficiency position favoring private-law regulation, then, is most likely valid where transaction cost (including information cost) is low. Validity will decline progressively as such cost rises. Such cost will rise for so long as the advantaged party, acting rationally, sets the default rules in its own best interest.

In seeking an optimal approach to the university application process, the efficiencies of bargain suggest themselves, particularly in light of the variety of implicated interests among school, applicant, and the various contributors to application files. Contract would permit creation of customized, negotiated expectations of privacy in the sense of permissible use.

In the admissions context, however, contract as an efficient general solution does not long withstand analysis, for two reasons. One is the

169. See, e.g., *Burch v. Second Judicial Dist. Court of Nevada*, 49 P.3d 647 (2002) (describing negotiating advantages of the home builder over buyers who were "not sophisticated consumers").

170. See POSNER, *ECONOMIC ANALYSIS*, *supra* note 27, at 115-18.

highly adhesive nature of admissions, rendering individual transactions inefficient, as just described. True bargaining in the highly adhesive admissions context is problematic in any event. Default rules set by schools would effectively be mandatory as to both primary and secondary employment of personal information accumulated in application files. The problem of excessive secondary disclosure would arise.

The other reason contract will not lead to efficient results under the present regime is transaction cost. To negotiate a privacy expectation with every applicant and every other contributor to every application file would result in insupportable aggregate transaction cost. The lack of uniform result would add further to aggregate cost. In this respect it is worth noting, again, that higher-education applicants have no right to see their own files and therefore cannot accurately value what they would be negotiating for in any event.

On a social basis, then, over the long run more would almost certainly be lost than gained by attempting to regulate control of application information on an individualized, private-law basis of negotiated exchange. In terms of social cost, we must look beyond individual negotiation.

The contract objective of fulfillment of expectations should not be abandoned, however. Indeed, because individuals' valuations of privacy vary so extremely, contract should be the positive basis of the application process. It best explains the behavior of applicants and schools. But for the expectation of purpose-informed limitation on use, applicants would not lay themselves so bare. Individuals do not lay themselves bare, incurring the attendant costs, for nothing in exchange and without conditions. Such a result is not likely to fall within a majority of individuals' reasonable expectations.¹⁷¹

Under the present admissions regime, provision of personal information is treated as a condition of entering the admissions process. This crucially overlooks the true exchange that occurs. Contract validates the value of an expectation of something occurring in the future. In the application context the applicant's expectation is the school's reasonable stewardship of personal information willingly disclosed. This is discussed further in the next Part.

V. A PROPOSAL FOR A NEW, COERCIVE DEFAULT RULE

In this Part, I suggest that the default rule for secondary

171. See *supra* note 38 and accompanying text.

employment of application-file information should be reversed—no secondary employment—and that reasonable care should be taken by schools to prevent file leakage. This should be an enforceable rule in the nature of a relationship of trust and confidence, recognizing the schools' position as stewards of their applicants' personal information.

This Article shows that the present regime regulating application files is innately inefficient. This inefficiency results from a convergence of factors: In the highly adhesive application regime, creation of a detailed and intrusive application file is a condition of application, not the result of an informed bargaining process between the applicant and the school. Applicants do not know and cannot know the value of the information that they are required to permit schools to accumulate. Applicants do not know and cannot know what secondary use may be made of application information. As a result of these two information failures applicants' personal information is undervalued. Like other providers of personal information, applicants will have a generalized expectation that such information will be limited to the purpose for which it was collected, and not be secondarily employed in ways costly to them. Unanticipated, excessive secondary employment inconsistent with this expectation is costly to the applicants. Applicants who know or believe that excessive secondary employment may result, and who are otherwise unable to self-protect, will rationally reduce the quality of their disclosure, and perhaps not apply at all. Accordingly, the highly adhesive regime that applicants face today is inefficient, costly to the applicants in terms of secondary employment of their personal information, and risky and costly to the schools in terms of admissions goals and reputation.

The current application-information regime is also inappropriate on a normative basis. Applicants and other contributors to admissions files provide information on the basis of an expectation of use and control pertinent to the purpose of the file. Such an expectation is reasonable on their part and is foreseeable by schools. If this is true, then the norm should be that the files' use and transmission should be regulated congruently with those expectations.¹⁷² If applicants do not trust schools' stewardship of the personal information provided them, this norm will be enforced by the applicants' degrading the accuracy and completeness of their application files.

To regulate the application information regime toward efficiency requires adjustment of the extreme information asymmetry of the

172. This is congruent with "fair information practices." See *supra* notes 71-72 and accompanying text.

application process. Because, in the nature of the process, applicants cannot know the value of what they provide to the schools, efficiency requires regulation of the schools' secondary employment in a way congruent with applicants' generalized expectation that their application files will not be used in ways costly to them or indeed in ways unexpected by them.

Applicants' expectations, and therefore efficiency, would be most likely to be served by shifting the positive basis of regulation of application-file content—the template, if you will—away from today's totally adhesive environment and toward exchange based on expectation—the schools' expectation of receipt of accurate information and the applicants' expectation that the information will not be secondarily employed in unanticipated, and risky, ways. The default rule should be the reverse of the present rule of disclosure: (1) that there will be no secondary employment at all; that is, that application information will be used solely for the purpose for which it was acquired; and (2) that schools will undertake reasonable efforts to avoid file leakage. This notion of exchange should be the common-law starting place, enforced as an *ex ante* deterrent to excessive secondary employment.

Schools that find significant gains in secondary employment could preserve them by negotiating around the default rule by describing to applicants what secondary employment they intend to make of application information and limiting secondary employment strictly to what is disclosed.¹⁷³ The terms proffered by the schools would be non-negotiable—the contract would be as perfectly adhesive as is the present regime and for the same reasons of efficiency in the admissions process. The difference would be that applicants' decisions would be informed as to how their personal information might be secondarily employed. A marketplace would operate in the sense that if applicants would decline to apply at schools whose offers were not acceptable.

What is described here is a coercive default rule,¹⁷⁴ designed to stimulate disclosure by the school, the party with the relevant informational advantage as to secondary employment. The rule needs to be coercive in the sense of compelling full disclosure by the school of its intentions of both primary and secondary employment, and to its steps to

173. Cf. Schwartz, *Property*, *supra* note 5, at 2082 (“Market-perfecting moves for the personal data trade would require removing or at least reducing information asymmetries between data collectors and individuals”); *id.* at 2095 (“[O]f greatest significance” is a combination of “restriction on the use of personal data combined with a limitation on their transferability.”).

174. Professor Murphy discusses coercive default rules in the text accompanying *supra* note 3. Professor Schwartz also refers to “information-forcing” default rules that “can reduce information asymmetries by placing pressure on the better-informed party to share relevant data.” Schwartz, *Property*, *supra* note 5, at 2082.

avoid inadvertent secondary employment.

Such a rule more accurately describes the positive nature of the transaction, which is exchange. Applicants would not have permitted these collections of personal information to be assembled outside their control but for the purpose of admissions analysis, an expectation in the nature of a bargained exchange. To describe the process as such recognizes that the applicants' expectations, including privacy preferences, have value.¹⁷⁵

For the school, the question then becomes whether the cost of precaution would exceed its efficiency gains. In my opinion, it certainly would not. Accurately informed applications are of the highest value to schools. Surely schools value more highly accuracy in application-file information and the maximization of the number of qualified applicants than they do the secondary employment of applicant information. As a long-time member of admissions committees, I cannot imagine any secondary employment of application-file information that would exceed the potential cost in terms of admissions goals and school reputation.¹⁷⁶

Schools would also benefit by engendering trust in applicants. Economics research shows that, in sharing personal information, trust is of "utmost importance" in order to persuade the subject to "accept the risk of the transaction."¹⁷⁷ Further, "perceived privacy and perceived security" are seen to be "the chief determinants [of] trust."¹⁷⁸ Trust, accordingly, should be of high value to schools in their admissions programs.

Such a rule would lower transaction cost across the board by enhancing predictability. It would promote accuracy in the information received from the applicant and other contributors to the file, and the

175. "Value" to the school, in my view, would adhere to any applicant's preference that would influence that applicant's behavior *qua* applicant. Thus, a pure privacy preference, with zero market value, would have "value" to a school if it stimulates an applicant to manipulate application-file information, or not to apply at all. My point in the text is that such value should be recognized even though it cannot be quantified. See Murphy, *supra* note 3, at 2293-96. Failure to so recognize applicant preferences will be costly to the school.

176. For those who would argue that it is efficient to use application-file information to inform what are, in effect, solicitations of donors (including, in the context of public institutions, members of the legislature), I would argue that such a practice should severely degrade a school's reputation for fairness in admissions, as well as its own admissions goals. I would extend this to making application-file information accessible to donors who contact the school or its staff or faculty to inquire about certain applicants. Such practices constitute indirect auctions of acceptances. I do not extend this point to the inclusion in application files of letters or other forms of recommendation initiated by donors, or to the sharing of application-file information with anyone who has obtained the permission to do so from the subject of the file. However, in those cases, it should be explained to the subject that such permission may result in the further dissemination of the shared information.

177. Chellappa, *supra* note 56, at 34.

178. *Id.*

applicant would be able to form more accurate expectations on which to base the decision whether to apply.

This rule allocates costs appropriately between applicant and school. File control is performed at least cost by the school. It is best positioned to put in place physical and electronic controls over the files themselves, and behavior controls over personnel. Secondary application and leakage cost to the student will be minimized at much lower cost than applicants could perform by monitoring or bargaining. In exchange the cost of supplying information will continue to be borne, appropriately, by the student, but the quantity and accuracy of the information should be enhanced, a value to the school.

A further incentive for self-regulation through a coercive default rule lies in the possibility of the imposition of government regulation. Opportunistic use of application information, or carelessness in protecting it, could entail cost by justifying government intervention and regulation with attendant cost in terms of administration and loss of local idiosyncrasy. Under the rule I suggest, remedies would lie in contract, not tort or breach of trust. Precaution in self-regulation is therefore well justified.

Remedies have been an issue for privacy-preservation schemes.¹⁷⁹ How are infractions detected and how are infractions valued? In the regime I propose, the privacy-preservation rule should be self-enforcing once schools understand the potential costs of the present regime. Increased awareness among applicants of the issues discussed in this Article should lead to market enforcement as well.

Schools should adopt appropriate policies and publish them to applicants.¹⁸⁰ Affiliated institutions, such as accrediting agencies, should encourage this.

Schools have great leverage to compel applicants and other contributors, such as writers of recommendations, to speak frankly through the medium of admissions files. I believe contributors do this with a reasonable and foreseeable expectation of limitation of use of such information to the admissions process. A regime of regulation based on expectation can only enhance the integrity and validity of admissions files, and therefore their usefulness for their declared purpose.

179. See generally Schwartz, *Property*, *supra* note 5, at 2107-08.

180. See Chellappa, *supra* note 56, at 36-37 (suggesting public education of the nature and risks of information sharing).

VI. CONCLUSION

I have used university applications as an example of the regulation of the collection of information in the context of a highly socially beneficial activity—so highly beneficial, indeed, that the relationship between school and applicant has been permitted to become extremely adhesive in favor of the institutional information collector. As demonstrated by the example of university admissions, these relationships have a strong propensity for inefficiency when they are so highly adhesive that one party can elicit private facts from another with no limits on secondary employment. Such relationships effectively are an exception to the usual rule of efficiency of disclosure, and, on account of transaction cost, fall outside the ambit of Coasean logic. Regulation won't be performed by the market because high adhesion is, in effect, a market failure. This generality can apply to many kinds of relationships in addition to school applications—parent-teacher associations, charities, children's sports teams, religious organizations, investment clubs, housing associations, buying clubs, retirement organizations, interest groups of various kinds—any sort of group that is of sufficiently high-value social and private benefit that it is able to demand, collect and maintain personal information, bringing to bear short-term market behaviors and rational ignorance—and that is not yet regulated by the government. The value of secondary employment is allocated as a windfall to the dominant party, while cost of excessive secondary employment or file leakage is allocated to the subservient party.

The inefficiency will come home to roost. The Yale/Princeton admissions-file hacking incident is an example, and the literature is filled with lists of disasters.¹⁸¹

This Article suggests that the regulatory answer is new starting places, coercive default rules bearing on the dominant party, stimulating surrender by that party of its information dominance. The positive basis would be contract, and reasonable expectations.¹⁸² Empirical inquiry shows that this is the norm.¹⁸³ A coercive default rule of no secondary employment would serve both efficiency and the indistinct privacy norm.

181. See, e.g., Fromkin, *supra* note 2, at 1501-05 (describing conflicts arising from information collections unanticipated by the subjects).

182. See Litman, *supra* note 8, at 1307-11 (observing that individuals experience "outrage" when secondary employment of their private facts exceeds their reasonable expectations). As Professor Litman notes, the Restatement contemplates enforcement of express limitations of secondary employment. See *id.* (citing RESTATEMENT (SECOND) OF TORTS §§ 892(2), 892A cmt. g.)

183. See Schwartz, *Personal Health Care*, *supra* note 2, at 44. See also *supra* notes 65-66 and accompanying text.