Introduction: Relationship between Free Speech and Privacy

by Tracy Mitrano

"Free speech" and "privacy" operate as integral, essential supporting values that underpin the missions of colleges and universities in the United States. Chapter One focused attention on free speech. Many of the same arguments could be made by and for privacy. It would be interesting to subject the same content about free speech to a global "find and replace" function for the applicable legal and policy points between them! Nonetheless, US law separates these two areas. Therefore, this chapter will focus on privacy law in particular: government surveillance and consumer privacy. Both subsets of privacy law, I will argue, have a profound impact on higher education. In turn, higher education's experience could and should have an equally profound impact on the law.

But first: the connection between free speech and privacy. As is well known, free speech was a key *explicit* issue in US law from the start. It is the first amendment to the Constitution and sets the tone for all of the Bill of Rights. Privacy was not. It is nowhere mentioned in the original Constitution, Bill of Rights, or any of its subsequent amendments. It shows up in Constitutional law as a part of dicta, or opinion, in the 1960s' cases involving family planning. While it has precedents in cases on essential liberties, the court in 1965 set its framework in the (in)famous "penumbra" of rights that the majority court found incorporating a number of the original amendments, specifically 1, 3, 4, 5, and 9. In civil law, Supreme Court Justice Louis Brandeis, as a young attorney, foresaw the need of torts to counteract the effects that new technologies such as photography were having on traditional upper-middle-class values. Wearing my historian's hat, and as I have argued elsewhere, founders did not explicitly identify privacy as a constitutional value, *not* because the culture had no sense of it – I would argue that it is as old as the human civilization – but because it was so intimately embedded in cultural norms that it did not require codification. Encroachment on cultural norms prompted prescient scholars such as Brandeis to give it legal definition. As law, privacy emerged increasingly in both civil and criminal law throughout the twentieth century as a result. As we move into the twenty-first century, and not least because of technology, we see it becoming of ever-increasing importance.

It is no coincidence that technology has been the driving force. From photography through telephony, birth control and abortion, technology is the persistent dynamic. The Internet has exponentially expanded and accelerated that development. Before diving into a deeper discussion of how the Internet – a combination of both market and technological aspects – has profoundly affected the social and legal landscape, it is worth explaining what the Constitutional does not protect. The constitution does not apply to Google, Facebook, or Amazon. These sites, and hundred of thousands like them, are all private. If compared to physical space, it is as if a user who visits these sites has "stepped" onto private property. Therefore, the user must abide by the rules that the company sets. For example, if I were to drive up to General Motors Corporation headquarters in Detroit, Michigan, I would be directed to a showroom someplace else. There would be no expectation that I could willy-nilly enter the grounds or walk around either its business or operational offices. The same is true for the Internet. If I go to the main Google search page, it is as if I were at the showroom. I am not invited into Google headquarters to be a part of its backline operations or its corporate boardroom where business plans are made or its laboratories where the code to its algorithm is tested or recalibrated.

Let's first examine how the private corporate entities of these sites affect free speech before turning to privacy. It is relevant to do so because free speech acts as something of a prelude to privacy. It also has a richer and more complex jurisprudence. For most users, the impingement on what users might consider their "free speech" may not be apparent. Facebook's "Terms of Service," for example, reserve the right to delete or block content, and it has done so in health and safety circumstances or when the expression becomes too vulgar or abhorrent ... in the eyes of Facebook. Given US law on obscenity, Facebook's standards are far more restrictive than are allowed under the First Amendment. Likewise, Google – or any other online service – can set its own rules. Social norms and the First Amendment are in sufficient alignment that the distance between the site's rules and what its users expect is not significant. Still, it is important to remember that it is this cultural alignment, and not the law per se, that protects speech on their site.

Administrative regulation, in comparison to Constitutional law, has its own effect. Unlike Constitutional law, which is limited to government action, administrative law is not. In fact, administrative law, as a broad category of law, exists in large part to moderate the adverse effects that the free market had on vital public policy issues in the history of the United States, be it in railroads, food and drugs, labor, or communications. Now that the Federal Communications Commission

has reclassified the Internet as a utility, rather than an information service, communication law prohibits telecommunication companies from discriminating with respect to content. In the course of the "notice and comment" that preceded the establishment of these rules, much was made of the speed by which packets would travel and whether, without reclassification, telecommunication companies would charge Internet companies exorbitant rates that would result in a differential user experience. In short, unregulated business models that preferred speed over content could effectively bring a site such as Netflix to its knees if it slowed to the point of user inconvenience. Thus, because technology has become the vehicle for speech, rules that affect speech are not decided by Constitutional law alone but through administrative process.

Not all users, even higher education administrators, appreciate these complicating factors that affect speech on the Internet. Confusion rests in the notion that the Department of Defense created the Internet. A series of Congressional acts opened the network system, which had been in development from the 1970s through the early 1990s, to the public. From these basic facts comes the assumption that the Internet is not only "free," but also public space. What is not understood is that the technical communications protocols, which move digitized "packets" of information through the medium, be it copper or fiber optical cables, aided and directed by "routers" and "switches" that interpret the Internet Protocol Addresses to get the data to its destination point, are in the public domain. Applications that resolve computer machine language into intelligible language, and sites that users visit, are not. The proprietary software that the company owns and deploys to create the site is protected under copyright. The point here is this: technical protocols, which are used to move content, are free for Internet Service Providers. That is a great boon to the telecommunication providers, who do not have to pay royalties to transmit content. But for the user, nothing about the Internet is free. The user pays for the Internet service via telephone, broadband, wireless data networks, or even satellite connections. The user pays for the devices that access the Internet. And, as we shall see, even if there is allegedly no direct cost to use a search engine or engage in a social networking site, the user does pay a price. That is what most distinguishes speech from privacy on the Internet.

Privacy Law in Historical Context

Prodded by market and technological encroachments on traditional social norms, privacy law has grown prodigiously in the last one hundred and twenty-five years or so. Moreover, it has grown in virtually every area of law: constitutional, criminal, civil, and administrative law. The expanse is so wide that it is critical to distinguish these areas. Below is a categorization that creates five distinct areas.

1. Family Planning, Reproduction, and Sexuality (Individual v. The State)

When a layperson first hears the word "privacy" in relationship to law, this area is probably -- or at least until recently, when the advent of the Internet fostered issues such as identity theft -- the first area that comes to mind. No wonder, because both the jurisprudence and the politics of this area have animated US society for a half century at this point. Before 1965, states could and did have laws that prohibited information about and possession of contraception. In that year, the Supreme Court decided that such laws violated the Constitution. Because the word "privacy" does not exist explicitly in the Constitution, the understanding among the prevailing opinions was that a "penumbra" of rights from Amendments 1, 3, 4, 5, and 9 amounted to such a right, contravened by states that imposed laws interfering with the decisions married couples made in their "bedrooms" about family planning. It was not long before the Court expanded the ruling from married to unmarried individuals, and then to a striking down of state abortion laws, and most recently to the decriminalization of adult, consensual sodomy laws, the unconstitutionality of the Defense of Marriage Act and, finally, with the help of the equal protection clause, same sex right of marriage.

2. Fourth Amendment and Criminal Law (Individuals v. The State)

The second area also readily leaps to most people's minds, especially in light of the USA-Patriot Act and TV series such as *The Sopranos* or the *The Wire*, in which there are dramatic depictions of wire taps. The Petraeus case and Edward Snowden's disclosures all point to this issue, as well as the newly minted "Freedom Act," which cabined some of the excesses of the USA-Patriot Act, but also has allowed government to continue with the secret Foreign Intelligence Surveillance Court. All of these laws and courts involve electronic surveillance. When first brought to the Court in 1928, in the context of a police wiretap on bootleggers' phones, the Court did not find a violation of the Fourth Amendment. Clamps on a black box did not resonate with the physical proximity picture of police entering an individual's home. By 1967, however, given much change in manners and mores (not least of which was the *Griswold* case, described above [this is not mentioned by name above], about making contraception legal), the Court reversed itself and found a Fourth Amendment right in telephonic communications.

The next year Congress passed a law that outlined rules, procedures, and consequences for "wiretapping," the 1968 Omnibus Safe Streets and Crime Control Act. In keeping with Fourth Amendment jurisprudence in physical space, it drew an important distinction between "content" and "conversational detail." The first, content, are the actual words spoken between parties on a phone conversation, preserved either as a recording or as a transcript and often used in evidence of criminal cases. Conversational detail, a misnomer in the sense that it is metadata and not the content of a "conversation," are telephone billing records. In 1986, Congress amended that law and passed the Electronic Communications Privacy Act (ECPA). The USA-Patriot Act, its many amendments, and now the Freedom Act have all amended ECPA in part, but at the time of this writing there has yet to be a comprehensive revision of this important cornerstone of privacy and due process rules for the Internet. In fact, that law, while at the time prescient in recognizing "data networking" as distinct from telephony, fails to track the Fourth Amendment according to the technological differences between them. ECPA conflates telephony and TCP/IP data networking in terms of legal process. As a result, ECPA in practice is the root cause of many legal uncertainties, such as the capture of all telephone metadata by the NSA and other questions of Fourth Amendment significance.

3. Public and Consumer Law (Individuals v. Corporations)
This third area has become familiar to the popular mind because they are confronted with it in the form of annual privacy notices from banks and forms to fill out before being seen by a doctor. The US has a relatively unique "sectoral" approach to public consumer privacy, by demarcating specific and narrow bands of information: for example, education records (FERPA); financial records (GLBA); health care records (HIPAA); and a series of other one-off categories, such as video rental records (as a result of the Bork nomination hearings and the disclosure that he rented pornography from Blockbuster). Europe and other developed nations, such as Australia, New Zealand, and Japan, have adopted comprehensive data laws that protect personal information in any context held by a company or a corporation. But in the United States, for example, only patient care records of a "covered" entity are actionable under HIPAA, not even all health care records. Cable subscription records are not protected but might reveal as much, if not more, about an individual than their bank account records.

4. Torts and Civil Law (Individuals v. Individuals)
Established at the turn of the last century, torts such as "misappropriation of likeness" or "invasion of privacy" have taken on real meaning for average people with the explosion of technology. Tyler Clementi's parents decided not to bring an action against the roommate who has faced criminal penalties for "invasion of privacy," but under New Jersey state law they could bring such a case. A cousin of "defamation" and "libel," these torts used to be reserved mostly for the famous. But as imaging and information technologies have grown faster than an appropriate use bounded by either case law or personal ethics, violations occur daily awaiting an angry plaintiff and a deep pocket.

5. Administrative Law (Corporations v. Consumer, mostly…)
Administrative law is probably the least understood area of law by most lay people because, while required to be transparent through "notice and comment rules," it is done by the executive agencies of the federal government. Sometimes called the "fourth branch," it is that area of law executed by, for example, the Federal Trade Commission or the Federal Communications Commission, the two agencies with respect to the Internet that are -- together with the Library of Congress, which houses the Copyright Office, and the Commerce Department, which controls the root domain name servers -- probably the most influential agencies for areas of the Internet. The Federal Trade Commission zeros in on privacy issues; it is the Commission that has and continues to press Google on the inherent ambiguities in its privacy policies. The FTC is also the agency that about a year ago required Facebook to inform its users of changes in their privacy settings. To calibrate the balance appropriately for economic growth and consumer safety, administrative law is a vital area of US law, and most especially on issues of privacy and the Internet.

****

Governmental Electronic Surveillance

In late October of 2001, I attended my first EDUCAUSE national conference. It was in Indianapolis. I immersed myself in all of the programs, sessions, and networking. Only a few weeks after the events of September 11, there was a lot to talk about. Not least was the impact of new legislation Congress was drawing up to address terrorism that included revision of existing laws on government electronic surveillance. And then it hit. On October 26, while we were still in Indianapolis, President Bush signed into law the USA-Patriot Act. Polley McClure, Vice President of Information Technologies and my supervisor at Cornell University, suggested to Brian Hawkins, President of EDUCAUSE, that I prepare a presentation. I borrowed two computers and burrowed myself into the hotel room.

On one computer I called up the legislation. On another, the legislation that it amended. And on a third, I took notes about what it meant. A couple of days later, on the last day of the conference, I presented to a small room full of people. Within the next six months, I gave variations of that presentation all over the country to about fifty different groups.

The USA-Patriot Act (Patriot Act) affected higher education in three specific ways. First, it amended the key privacy legislation that affects colleges and universities -- the Family Education Rights Privacy Act (FERPA). Promulgated originally in 1974, FERPA protects the education records of students from indiscriminate disclosure. As is the case with every privacy law, exceptions apply. FERPA already included exceptions such as a proper showing of law enforcement, emergency health and safety of the student and at the student's request or consent. The Patriot Act added a terrorist exception designed to protect the "health and safety" for everyone else. In the case of a potential terrorist threat, law enforcement can acquire education records. Importantly under this exception, the threshold law enforcement had to meet was much lower than in any other case, including as a matter of criminal law which comported with the Fourth Amendment. Thus, rather than probably cause of criminal activity, law enforcement was only required to show connection to an investigation of terrorism.

The second way in which the Patriot Act affected higher education was not directed onto higher education but was rather in the more general area of electronic surveillance. To understand its impact requires analysis of the state of U.S. electronic surveillance law even before the Patriot Act. Electronic surveillance law is encapsulated in the Electronic Communications Privacy Act of 1986 (ECPA). A revision of the first U.S. electronic surveillance law, the Omnibus Safe Crime and Streets Control Act of 1968, ECPA prospectively included data networking in its scope but failed to take account of the technological differences between Internet and telephone protocols and how those technological differences map to the Fourth Amendment. The revisions of ECPA resembled in effect the one for FERPA: a lowering of the bar by which the law enforcement could obtain otherwise protected content.

Under telephony, ECPA distinguished between "conversational detail," or "metadata," and content. (The original term was conversational detail. Metadata has replaced that term, in large part as the dominant form of communication has shifted from telephony to the Internet. I will therefore use the term metadata for both forms of technology.) For example, with telephony, metadata is the source and destination number time stamped. For data networking, a name for the packet-switching technology of the Internet, metadata is usually source and destination Internet Protocol address for another computer, such as for email, or the server of a web page, such as in an Internet search.

Mapped to the Fourth Amendment, metadata under telephony comported well with the distinction between the business information about the call and the actual verbal content of it. Under ECPA, a subpoena is required for the former, and a warrant for the latter. Subpoena power derives Constitutionally from the commencement of a case in court; each party has the power to get the information it needs in order to makes its argument. A warrant is also driven by the Constitution. In this case, it is the Fourth Amendment that requires law enforcement, and only law enforcement -- NOT a party in a civil suit and therefore only in criminal cases -- to persuade a judge of probable cause of criminal activity to allow, for example, a phone line or Internet connection to be tapped for actual content.

The different nature of the technologies is the fly in this ointment. This rubric works well for telephony, where the law and technology are in Fourth Amendment alignment. It does not comport to the Internet, however. Given that an Internet Protocol address can be resolved to content, a web page for example, means that the law and the technology are not aligned as a matter of fact. For less that probable cause of criminal activity, law enforcement through a subpoena, not a warrant, could have access to content. Moreover, advanced algorithms when combined with metadata have collapsed the legal distinction between metadata and content in a manner that has rendered ECPA anachronistic. (There are other ways in which this law is also very much outdated, the subject of which is not in scope for discussion in this context, however.)

The Patriot Act delivered a final punch in what was already legally problematic. With respect to metadata, it lowered the requisite subpoena power that comes with the commencement of a case to a procedural matter as simple as filing a letter with a clerk. While some observers might suggest that this distinction is one without a difference, it is nonetheless one that comes at the expense of a potential defendant. No judicial oversight combined with content that data networking metadata can reveal means that a person who falls under law enforcement's suspicion has virtually no legal safeguards to governmental surveillance. This state of affairs for Title III criminal courts and does not even take into account terrorist investigations that come under the "secret courts" of the Foreign Intelligence Surveillance Act.

The third way in which the USA-Patriot Act had an impact on higher education concerns its amendments to the Foreign Intelligence Surveillance Act of 1978. The Foreign Intelligence Surveillance Act originally acted as a break on overseas clandestine activities of the U.S. government. It did so by bringing some form of legal process to Central Intelligence Agency (CIA) actions off the Constitutional radar. The creation of a secret court, known as the FISA Court, seemed a reasonable means to balance the need for secrecy with the need for some judicial oversight. At the time, the notion of a secret court, and notably one that is *ex parte*, which means that the government is the only party to the court, there is no attorney for the defense -- did not shock the conscious of the American public because its work was thought to be exclusively on or about foreign soil, where the rights of citizens under the Constitution do not even obtain and therefore the court did not need to comport to the Sixth Amendment (which lays the foundation for the judicial system in federal criminal court.) Globalization in its myriad technological, market, political and cultural forms began to crumble the wall between what was foreign and what was domestic almost from the start, however. By the time that Edward Snowden make his revelations about the collection of telephone metadata of everyone in the United States – a practice that was begun the day after 9/11 by executive fiat and was made ostensibly legal in 2008 with the FISA Amendment Act -- was it clear that for all intents and purposes, the wall had collapsed.

The USA-Patriot Act further loosened the strictures of the FISA Court. First, it allows for the collection of information on persons who are "significant" to an investigation of terrorism. This standard is well below the Constitutional standards by which we operate criminal courts in the United States. It opens the proverbial floodgates to a potentially infinite number of persons who can come under surveillance. And in fact as the Snowden disclosure revealed about collection of telephone metadata, that is exactly the case. According to the legal standards by which FISA operates, everyone in the United States must be a person significant to a terrorist investigation!

Second, the Patriot Act gave the FISA Court the authority to issue "national security letters." National Security Letters require an entity in control of metadata to supply it. Such entities include colleges and universities that act as Internet Service Providers. If the whole FISA framework were not problematic enough for a college or university to have to respond to such a request, an automatic gag order that accompanies this request made the prospect especially objectionable. Not only does the college or university have no court to which it can appeal if it wishes to challenge the request, the institution is not even able to report out the fact of it. The court of pubic opinion is also closed off. For rules not of their own making, colleges and universities seem structurally complicit in this obvious Constitutional conundrum.

In addition to the National Security Letters, what has become known as section 215 of Patriot Act raised higher education's hackles, especially those of academic librarians. Known generally as the "business records" provision, section 215 allowed again through the channels of the secret FISA court law enforcement to collect a wide swatch of information about individuals without the benefit of Fourth Amendment jurisprudence. And once again, the Snowden disclosures bring the concerns of academic librarians, among others, full circle. It was specifically under this provision that the National Security Administration made its request to the FISA court to collect all telephone metadata even of people in and the citizens of the United States.

Impact of Electronic Surveillance Law on Higher Education

What impact do these irregularities in the law of government surveillance on Internet technologies have on higher education in the United States? In practice, for the most part, it would not seem to amount to much. Research continues apace. Faculty and students – less so staff, for obvious reasons of their status – speak out in classrooms, on site, via both campus networks and publicly on the Internet. Can anyone document a single case where a researcher or a student has had his or her academic missions compromised as a result of government electronic surveillance? Probably not. If there have been such cases and it involves terrorism, we may either not know about it, or, as institutional administrators, we may not be allowed to discuss it! But in the main, is there anyone in the academy who can honestly say that their research, teaching, or learning has been adversely affected because of a governmental encroachment on their privacy? I should like to meet such a person. And yet, I am sure that many exist.

Neil Richards, a law professor at Washington University Law School in Saint Louis, makes a compelling case for precisely this point in his important book *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age.* Admittedly, his focus is more on civil privacy than on criminal or governmental surveillance, but the connections he makes between free speech as a constitutional matter – and therefore governmental – and privacy, and then between privacy and autonomy of person and thought, speak universally to the founda-

tional principles at stake. Institutional missions of higher education require a minimum degree of both individual and institutional autonomy in order to meet the essential goals for which these institutions exist: transmission of culture from one generation to the next; the spurring of original thought and innovation to refresh each generation with new and stimulating material for every facet of life from ideology through to economic rejuvenation; the cultivation of citizenship values, both national and increasingly global, in an international marketplace. As a public service to US economy, society, and politics, higher education must have free speech and privacy – or, as Richards would have it: intellectual privacy – to function in research, teaching, and outreach.

Richards did not make his case for higher education specifically, but I will. In fact, higher education makes his case. Without individuals and institutions devoted to public service goals in a free market society, which legitimates self-interest as a preference in the ordered liberty balance, there may not be a clear-eyed appreciation of intellectual privacy's significance. This prioritization of higher education may strike many as off balance. Isn't the place of higher education supposed to be supportive of a vibrant economy, social mobility, and political participation rather than at the forefront? Were we back in the eighteenth century founding the republic, transforming myself as entitled to citizenship and therefore a voice, I would say yes. I would agree because I would accept the racial, class, gendered (to name the big three categories) social order as a given foundation upon which the citizen could function well as legally free, propertied, and privileged. Higher education as it existed then, largely as formation for clergy and refinement of the upper and rising middle class of that era, was not what it became in the middle of the twentieth century, to quote Senator Fulbright, who riffed on President Eisenhower's revealing presidential farewell address, a part of the "military-industrial-higher-education-complex." What observers have failed to appreciate is that, in the kind of conservation of mass and energy that exists in social dynamics, something has to proverbially give once you loosen the bonds of the categories upon which previous social orders are built. Of course, in human experience no experiment is as neatly controlled as that in a laboratory of science, but the basic point remains. Twenty-first century US society, determined against the odds to advance non-discrimination and equal opportunity, no greater sector than higher education exists that represents our founding father's values and promise.

It is therefore all the more imperative that privacy in all relevant aspects -- not least in communications and speech, learning and research -- be protected from any form of encroachment. In fact, it is precisely privacy, once embedded in social norms and newly encoded in law, that is the prerequisite to speech. Without privacy of thought, free speech has no grounding. One might be free to speak, but without recourse to the personal formulation of ideas, the speech may be of little or no importance. A mere recitation of what one has already heard through existing media channels, designed and shaped largely for corporate interests, parrots but does not advance society in any real sense. Higher education distinguishes itself from the culture at large insofar as it is uniquely tasked with fostering critical thinking. As such, it may be the last vertical [vertical what?] in US society that neither needs nor should not hold itself hostage to popular media trends. Rather, it exists to examine those trends as part and parcel of its radical – as in root – exploration of all aspects of nature, culture, and human experience.

Of course, exceptions exist even to this vaulted principle. As a professional drafter of rules for many years as a policy director for a major corporation -- Cornell University – as well as an observer of law in the United States for professional reasons of compliance, in addition to internalized obligations of citizenship, I have come to appreciate that any law or policy that is worthy of its weight in enforcement will always have exceptions to it. Privacy is thus. National security, criminal activity, health and safety, utilitarian research, and personal consent – to name a few of the obvious exceptions – all have their place. Tied together appropriately with "due process," these exceptions are what make the notion of a rule of law a functional reality in a reasoned and ordered society, no matter what its historical or cultural challenges. Adaptability to new circumstances is the trick to keeping a rule of law fresh, however, and that is where the United States has been unduly lax. Some lag between the launching of technological innovations and creation of laws in keeping with those innovations and the market practices and social norms that they face is inevitable, at least in a society intentionally governed by the market. But a lag that begins to hamper the market or peck away at the foundational values of a society is a symptom of some larger dysfunction. The subject of another book, that dysfunction is nonetheless contributing to the threats that undermine our colleges and universities. A political order that can't get its Fourth Amendment jurisprudence straight, within an economy driven by the information technologies that it created in the first place, is a country burdened by incumbents who are more concerned about carving out their personal gains in the present than in how to prepare the society for the future global economy our children face.

Customer and Consumer Privacy Law in Higher Education: Google Apps for Education

Government surveillance is not the only type of privacy law that affects higher education. Consumer, and in the case of enterprise systems customer, privacy law constitutes a very significant aspect of what higher education must countenance in this new information economy landscape. In fact, I would argue it is the most important of all the areas, including government surveillance. I make that point because, while I believe deeply that Fourth Amendment jurisprudence has a direct and immediate impact on higher education's missions, I cannot report specific cases of its effects. With consumer and customer aspects I have direct, and very troubling, experience.

In the last several years, new consumer and in some case customer services have emerged for file-sharing, storage, and social networking such as Gmail, DropBox, Twitter, Skype, YouTube, and Facebook. The notion of services for "free" has encouraged their popularity with users. How these companies use personal data is not well known nor understood, even by savvy digital users, however. "Click-through" Terms of Service, which consumers neither read nor understand, give these companies permission to do just about anything they want with that data, including profiling individuals, selling the data, or using it for increasingly sophisticated marketing and targeted advertising. To appreciate fully the nexus between technology and the market is to make sophisticated connections between the value of data and a global information economy fueled largely by marketing, advertising, and user profiling.

The underlying business model for these "free" services is a three-step process. First, an Internet company embeds code in web pages for keeping track of web sites visited, posts made on social media sites, products purchased, locations visited (based on mobile device location services), and many more attributes associated with an individual's online actions. All of this information is combined into a personalized online profile. Internet companies typically auction space on websites and in search engines so that an ad is matched to the user's interests. Payoff to Internet companies occurs when the user clicks on the ad.

Second, with search and online profiling, the marketing can be much more targeted. The more the Internet company knows about a specific user, the more effective the ads. Likewise, the more sites, services, or even devices controlled by the Internet company, the more information that can be gathered about the user, making the ad-matching service increasingly effective. Expanding reach is critical for these online marketing companies. Third, in order to attract more users, these companies will build more services and make the services "free" to garner ever-increasing amounts of personalized data. Revenue-earning potential expands as a function of that information and has, overall, become the standard business model for the most profitable and popular Internet companies.

Concurrent with the rise in popularity of these consumer applications is the emergence of enterprise cloud computing. Enterprise cloud computing delivers services such as storage, email, document creation, collaboration, and other programs through Internet companies that hold the infrastructure, applications, and the data on their own premises to contracting parties, including colleges and universities. For educational institutions, cloud computing has real benefits, especially in the areas of reducing cost, overhead, and staffing. Colleges and universities contract directly with the vendor for the services. Central to those contracts are provisions that explicitly require compliance with federal law to protect education records under the Family Educational Rights and Privacy Act (FERPA). The vendor promises to act as a "school official" by not disclosing a student's education record apart from recognized statutory exceptions, such as health and safety of the individual student.

A key point in these relationships is the respect for the institution's statutory obligations and the students' privacy. In practice, that means that at no point does the cloud provider have a legal right to use and/or resell education records for its own commercial purposes. These school-vendor relationships are purposefully designed to meet the mission-driven needs and compliance obligations of not-for-profit higher education.

Internet companies and educational institutions must be clear with each other in negotiations and contract formation about the technological and business practices of enterprise cloud computing. With a consumer "click-through" license, the end user assumes the risk of disclosure; whereas, with an enterprise contract, students place their trust in the institution that it will protect their privacy. Embedded in that trust relationship is the public policy recognition of the vulnerabilities particular to the age and stage of development of students. Students require privacy to learn from mistakes without fear of exposure or embarrassment. Speech and curiosity could so easily be chilled if a person thought that something they did or said while in that critical formative process could later in their life be used against them. Within this protected zone to develop strong intellects and open hearts lays the hope that a student may grow into a well-educated, productive

member of the economic workforce and a vibrant citizen in our democratic society.

The Family Compliance Privacy Office of the Department of Education has made two points clear regarding cloud computing. First, colleges and universities cannot ignore their obligations under FERPA by outsourcing the processing and handling of education records to third-party vendors. The obligation follows the records, and the institution remains responsible for its vendor's compliance, which should be made clear in the contract. Second, data-mining or any other use of education records for the vendor's own purposes – including, but not limited to, advertising and other commercial purposes – is a per se violation of FERPA. Thus, it is critical that colleges and universities have sufficient transparency regarding the technologies and business purposes vendors put to the education records under their control. Informed consent rests on this knowledge, as does the responsibility that educational institutions assume to contract on behalf of students. Ad-revenue, subsidized services are neither legal nor appropriate for educational institutions. An Internet company that mines education records for its own business purposes acts against both law and public policy.

While in my experience some companies have recognized the need for compliance and have respected those rules in both contract formation and technological/business practices, for example when Box worked diligently with representatives of a number of pilot institutions in the original Net+ contract formation, others have ignored those obligations, obfuscated reasonable inquiries, and deceived contracting educational institutions. Under those circumstances, it is impossible for the college or university to exercise informed consent. One company that played a duplicitous game in this outsourcing space was Google – the world's largest online advertising company.

Why focus on Google? The answer is in many ways obvious: it is the most economically powerful and technologically advanced Internet company in the world. Google is not only a $50+ billion-a-year online advertising powerhouse, it is also the dominant online search provider; the dominant player in mobile platforms (with its Android); a leader in online email services; a major player in mapping services (Google Maps); online video (via YouTube); web browsers (via Chrome); and numerous other online services. Of late, its business developed into the creation of a new entity, Alphabet, which acts as the corporate shell and parent to the original publically traded, for-profit company that formed out of the innovative and enterprising efforts of Larry Page and Sergey Brin.

Before the creation of Alphabet, Google inserted itself into higher education with both promise and alacrity. Beginning with its Google Books project, and then continuing with cmail and then Google Apps for Education (GAFE), Google appeared first as a partner to higher education, a knight in shining armor that would take over the reigns of organizing the world's information at precisely the time that higher education was being saddled with burdensome operational costs, reduced funding from the government and mounting tuition price that angered students and parents alike. These compromising circumstances only became more acute as the economic downturn of 2008 reduced even the prodigious endowments of well-heeled institutions. Boards, presidents and provosts began to look to see from where the sky-rocketing expenditures were coming and understandably zeroed in on information technology. Few put that identification in the context of an altered global information economy, or compared that expenditure to other verticals such as health care, to see that higher education was no different from any other sector of global society that made similar investments. Turning inward, institutional leaders tended to make a simple declaration: cut those costs! In rode Google with "free" services on a white horse.

There would be much to celebrate and little to criticize if a court case completely separate from higher education had not exposed a critical flaw. Two strike lawyers looking for a gold mind brought a case against Google in their hometown in Texas. The "strike suit" alleged that Google's Gmail data mining technologies violated the ECPA. In an effort to swat the gnat dead, Google moved to change venues to its own backyard in Silicon Valley. That move proved successful, but a skillful, smart and no-nonsense Judge Koh allowed the case to survive Google's second summary judgment motion. A summary judgment motion means that assuming all the facts in favor of the opposing party, there is no legal issue to try the case. Of the belief that motion would be a slam-dunk in their favor, Google suddenly found itself moving onto the discovery phase of the litigation.

What emerged in the course of discovery had more resonance for Google's enterprise clients than it did for consumers.

Federal District Court Judge Lucy H. Koh explained the plaintiffs' claim:

"After [date redacted], Google separated its interception of emails targeted for advertising from its interception of emails for creating user profiles. As a result, after [date redacted], ***emails to and from users who did not receive advertisements are nevertheless inter-***

cepted to create user profiles*. Accordingly, these post-[date redacted] interceptions impacted all Gmail and Google Apps users, regardless of whether they received advertisements."* [Emphasis mine]

While ad serving and user profiling are distinct processes within Gmail, until 2010 they operated at the same point in the email delivery process, since both were triggered only after an email was actually opened. But by 2010, Google realized that tens of millions of users were escaping the user profiling process, known as Content OneBox, because they used versions of Gmail, where for one reason or another, the ad-serving process was disabled or absent. Some of these users were accessing Gmail through smartphone apps, which didn't display ads due to their limited screen size. Others were using GAFE which did not serve ads by default. Google therefore decided to move the Content OneBox profiling process upstream in the email delivery process to a point before the actual delivery of messages to user inboxes. Thus, as revealed in court documents, sometime between September-October 2010 and forward, all inbound Gmail messages were analyzed for user profiling purposes before they were delivered to users – regardless of whether these users were being served ads or not. This meant that messages sent to smartphone users and GAFE users would be analyzed in just the same way as ordinary Gmail messages. Indeed, Google even began to analyze messages that users themselves deleted without opening.

This distinction between serving ads and data-mining/profiling has proved nettlesome in the history of enterprise contracts with schools, colleges, and universities. First, Google offered only "contracts by URL," meaning that the substantive provisions in a contract remained at Google's discretion to change without notice to the college or university. Data-mining and profiling practices were never mentioned in those contracts, or even in their URL statements. Instead, something of a linguistic shell game emerged. If representatives of a colleges or universities negotiating with Google asked about its data-mining/profiling practices, Google's stock response promised not to serve ads. If legal counsel or chief information technology officers had some concern about the nexus between "ads" and data-mining/profiling, negotiations with Google did not allow those concerns to be fully expressed or adequately explained. In the main, Google offered only sales people to discuss the contracts, not lawyers, even after college and university attorneys emphatically insisted on such discussions. In many of the earliest cases, the failure of Google to bring lawyers to the table resulted in contracts that did not even include FERPA provisions. Under pressure from institutional counsel to include that language, Google eventually added those provisions but still failed to provide either counsel or chief information officers with sufficient information by which to allow these representatives to exercise informed consent for the service with respect to FERPA.

Were it not for the chink in Google's armor that the discovery process of the Gmail litigation yielded, one might chalk these discrepancies up to the gaps that emerge in periods of rapid technological and business transformation. The documents that emerged from this case confirmed the suspicions of many chief information officers and institutional attorneys regarding data-mining and business practices in GAFE contracts, however, consistent with Google's established pattern of purposefully forging ahead of existing law. Precisely to the point of their concerns, the judge in the Gmail litigation, Judge Koh, ruled that:

"Google points to its Terms of Service and Privacy Policies, to which all Gmail and Google Apps users agreed, to contend that these users explicitly consented to the interceptions at issue. The Court finds, however, that those policies did not explicitly notify Plaintiffs that Google would intercept users' emails ***for the purposes of creating user profiles or providing targeted advertising****."* [Emphasis mine]

Thus, in March 2014, with pressure building, Google publicly acknowledged that it was indeed scanning the emails of GAFE users for ad-related purposes, but refused to deny that it also profiled students in GAFE:

"A Google spokeswoman confirmed to Education Week *that the company "scans and indexes" the emails of all Apps for Education users for a variety of purposes, including potential advertising, via automated processes that cannot be turned off—even for Apps for Education customers who elect not to receive ads.* ***The company would not say whether those email scans are used to help build profiles of students*** *or other Apps for Education users, but said the results of its data mining are not used to actually target ads to Apps for Education users unless they choose to receive them."* [Emphasis mine]

Shortly thereafter, on April 30, 2014, Google published a blog post announcing that it would discontinue "ads scanning" in GAFE contracts. This statement came without any additional explanation despite a statement that Google made just a few weeks earlier that GAFE ad scanning is "100% automated and can't be turned off ":

"We've permanently removed all ads scanning in Gmail for Apps for Education, which means Google cannot collect or use student data in Apps for Educa-

tion services for advertising purposes…. We're also making similar changes for all our Google Apps customers, including Business, Government and for legacy users of the free version, and we'll provide an update when the rollout is complete."

Google's statement that it had "removed all ads scanning" was notably silent on profile scanning. Once again, Google transposed language about "ads" to cover up data-mining technologies and commercial use of education records. Additionally, Google did not mention that, when enabled by an institutional technology administrator, the GAFE toolbar contains both enterprise and consumer apps, such as Gmail and YouTube, respectively. As a result, GAFE users may leave the protected enterprise environment and enter consumer applications not covered by their school, leaving them subject to ads and related scanning without receiving notice or the opportunity to opt-out.

This case highlights Google's misrepresentations to colleges and universities. It demonstrates that Google did not provide higher education with requisite information about its technological and business processes. Google stripped its enterprise users meaningful informed consent and made it impossible for educational institutions to determine whether Google would, could, or did meet regulatory obligations. Google did not serve proper notice or provide opt-out provisions related to its email scanning processes for the purposes of targeted advertising and creating user profiles. It refused institutional counsels' requests to negotiate in-kind with Google attorneys. It offered "contracts" that are not proper contracts under the Uniform Commercial Code (UCC). Those documents operate by changeable – and frequently changed – URLs. Indeed, to date Google continues to offer contracts to colleges and universities that, no matter what the provisions state, nonetheless include a fail-safe "out," a default reference to their ***consumer*** Privacy Policy. In other words, Google builds in layers upon layers of excuses and prospective defenses to their on-going pattern of deception.

Google obfuscated a clear response as to whether it data-mined education records for its business purposes of profiling. It transposed policy about its use of ads to cover up clear answers about profiling. Finally, it deceived GAFE users. For years, Google made a clear promise on its website stating, "Note that there is no ad-related scanning or processing in Google Apps for Education or Business with ads disabled." Google removed this sentence from its website in the same month that the Gmail litigation revealed allegations that Google scanned all GAFE messages for user profiling, even when no ads were served. The utility of the linguistic shell game had finally lost its ability to deceive administrators, faculty, staff, and students of U.S. colleges and universities.

No matter how much we all might value innovation, it is not worth the damage incurred through this deception. No matter how much we enjoy the fruits of an economy enlivened by the Internet, it is not worth the cost of undermining essential principles of American society that prize privacy as a prerequisite to personal autonomy. In taking advantage of higher education, Google has demonstrated a willful indifference not only to the privacy of the individuals in these institutions, the representatives of the institutions that have acted in good faith on their behalf, but also of the public service mission that higher education has to U.S., if not global, society overall. Assuming – and it is a considerable assumption given previous deceptions, but nonetheless assuming -- that the practice of profiling is no longer done on enterprise contracts within the Google ecosystem of GAFE, the Google experience represents an object lesson in how significant both consumer and enterprise customer privacy remains for higher education. This experience also forces the question of whether the federal government, the Federal Trade Commission and the Department of Education in particular, might be in service of higher education's missions when set against powerful corporate titans against whom higher education, at this stage of its history, can neither call on the carpet nor compete.

Privacy Torts and Higher Education

The fourth area of privacy outlined earlier in this chapter concerns privacy torts. The origins of these torts in the famous 1890 Samuel Warren and Louis Brandeis need not be repeated here. As an oft-told tale, it is well represented in the literature. Why it is told so often is worth a comment, however. In our Anglo-American law that relies on culture and tradition and which goes back so many centuries, it is not often that one can pinpoint a precise moment at which a whole, new area of law emerges to take shape. Indeed, the entire "Law of the Horse" notion rests on the idea that nothing new occurs under the sun, and existing law grounded in this venerable tradition need only be applied to contemporary circumstances. Warren and Brandeis, writing long before Frank Easterbrook, would not have agreed with him. What was so startling about what they did was to create new law as a response to new circumstances. Market and technology forces, which so profoundly unsettled social norms, motivated this legal development.

I predict that it will grow apace throughout this century. The information-political- economy, spurred by rapid technological developments, have assumed the proverbial baton that photography and mass publishing handed to digital technologies and networks in the last century. If the social norms of the privileged in the late nineteenth and early twentieth centuries prompted Warren and Brandeis to introduce a new category of law, as Neil Richards among others have suggested, then it was just the beginning of how pervasive and thorough technologies would encroach on all classes of the society and take over as the prime driver of the market as it transitioned from industrial to information in the last quarter of the twentieth. Medical science began the march with family planning law that brought privacy into the constitutional context. Much of information technologies can explain the development of law in the other four areas I addressed: electronic communications, information privacy, privacy torts, and federal governmental regulation of the excesses of an information market economy on consumers.

In the last section I made the argument for a Federal Trade Commission investigation of Google in its enterprise contracts with higher education. As of this writing, and news about the reluctance that the FTC has to initiate such an investigation, I turn now to the novel question of whether it is possible for higher education to bring privacy tort action against Google for the same practices that I have already described: in short, violation of enterprise contracts that promised colleges and universities protection under the Family Education Rights Privacy Act. Moreover, that it violated the privacy of the institutions and the individuals by not disclosing what it was doing with the information it gathered, and how it used that information to pursue its own profit and business model on the Internet.

I am not a litigator; I did not go to law school to practice. But I challenge those who are with interpreting these torts in light of the Internet in general and the practices of Google in particular. Novel circumstances create novel law. Not only is privacy law new in the United States, but also the forces that motivated legal scholars to create it in the first place have both shifted upward in significance and accelerated in pace with the associated facilities of network systems, myriad desktop and mobile devices, sophisticated software algorithms, a new market for behavioral advertising, targeted marketing, new Internet business models, and a tremendous new consumer as well as enterprise customer base. Who, in short, will be the Warren and Brandeis of this generation to pioneer new law and find their story oft told in the next generation of observers of law in cyberspace?