FACEBOOK’S RADICAL TRANSPARENCY: 
THE ETHICAL IMPLICATIONS FOR PRIVACY IN AMERICA

A Thesis
submitted to the Faculty of
The School of Continuing Studies
and of
The Graduate School of Arts and Sciences
in partial fulfillment of the requirements for the
degree of
Master of Arts in Liberal Studies

By

Donna W. Rohrer, B.A.

Georgetown University
Washington, D.C.
October 26, 2012
FACEBOOK’S RADICAL TRANSPARENCY:
THE ETHICAL IMPLICATIONS FOR PRIVACY IN AMERICA

Donna W. Rohrer, B.A.
MALS Mentor: Gladys B. White, Ph.D.

ABSTRACT

Facebook was founded by Mark Zuckerberg on the radical social premise that transparency will permeate modern life and will be a force for social good. However, what Facebook actually accomplishes is not as benign as its founder envisions. The social networking site’s continual introduction of features that encourage millions of users to share more data about themselves online with an ever-wider network of ‘friends’ poses an intriguing ethical question: What will be lost if privacy is no longer there?

Although the global transparency movement offers benefits to people struggling to obtain greater freedom from oppression in all its forms, it also brings perils, as transparency is used as an instrument of control and power over people. The answer to the question is that without privacy, which is derived from and essential to basic democratic liberties, including freedom of expression and freedom of the press, there is no modulating influence on the disruptive invasions that Facebook and other Internet providers can wreak on personal dignity and autonomy. The European Union approach to privacy illustrates principles that can be applied to restore balance among sometimes competing rights in America, both for individuals and the larger social good.

Facebook’s radical transparency requires that policymakers adjust the levers among the four ethical constraints that define the Internet, as Lawrence Lessig first identified: law, market forces, social norms, and the architecture, or code. The social
goods and individual human flourishing that privacy enables is essential to balancing the panopticon effects of such Web 2.0 practices such as, data aggregation and storage and data mining.

Remedies to restore equilibrium include application of privacy enhancing technologies (PET) to give citizen-consumers tools to better control access to personal information, policies to incentivize Internet businesses, and rules to establish the principles of limited use, expiration dates, contextual integrity, and the pluralist social values that will sustain civility and community in the information age.
The research and writing of this thesis is dedicated to
my advisor and mentor on cyberethics, Professor Gladys B. White, Ph.D.,
for her clarity of thought and patience of spirit,
and to my thesis editor, Richele J. Keas, M.A.,
for her sparkling good humor and sharp digital pencil.
# TABLE OF CONTENTS

ABSTRACT ..................................................................................................................... ii  
DEDICATION ................................................................................................................ iv  
INTRODUCTION ........................................................................................................... 1  
CHAPTER ONE  
LEGAL AND POLICY PERSPECTIVES ON PRIVACY IN AMERICA ..................... 4  
Technology’s Impact on Privacy Law and Policy ...................................................... 7  
The Judicial Legacy of Privacy ................................................................................. 9  
Privacy Policy Since 2000 ....................................................................................... 17  
CHAPTER TWO  
THE VALUES OF PRIVACY IN AMERICA .............................................................. 26  
Normative Conceptions of Privacy ......................................................................... 28  
Privacy’s Value to Society ......................................................................................... 35  
Social Norms About Privacy ................................................................................... 40  
CHAPTER THREE  
FACEBOOK’S RADICAL TRANSPARENCY AS A SOCIAL NORM ....................... 47  
Foundations of Transparency .................................................................................. 51  
The Promise of Transparency .................................................................................. 56  
Perils of Radical Transparency ................................................................................ 60  
CHAPTER FOUR  
PRIVACY: BALANCING FREEDOM AND AUTONOMY ..................................... 70  
European Views of Privacy ..................................................................................... 72  
Lessons and Options .............................................................................................. 81  
Current U.S. Policy Direction ................................................................................. 88
INTRODUCTION

On a day in January 2012, a Google search returned more than 6 billion references to the word “privacy,” almost three times more than a watch word of post-9/11 America – “security.”

Small wonder. Privacy is an important topic these days. Every business that touches the Internet has a privacy policy, most probably captured in Google’s galactic grasp. In America, citizens presume their privacy is protected in their homes – behind walls and locked doors and curtained windows – from prying eyes and ears. And based on that venerable assumed right, many Americans still expect their privacy is somehow protected when they go online to chat on Facebook, or send an e-mail, or order a video to watch at home.

The reality, however, is that personal privacy is far from assured. It is in fact a murky business once citizens leave the invisible boundaries of their domiciles, and enter this new digital world of global business transactions, social networking, and digital commerce.

Privacy is complicated, with more variety than one might suppose in how it is defined, applied, and protected by law and social norms depending on where you are, who you are, and what you are doing – especially when you are doing something in the digital world that increasingly shapes how everyone lives and works.

Despite these complexities, the subject is considered so important that the 112th U.S. Congress is looking over no fewer than 20 bills concerned with where legal privacy boundaries should be in such areas as: giving parents the ability to control their children’s
use of social media, and penalties for online businesses that allow children to access their sites; and rules that prohibit employers from requiring access to employees’ social media accounts or making employment decisions based on social media postings. Today’s Internet giants, from Facebook to Google to newcomers like Pinterest, are being forced to defend – and in many instances alter – their privacy policies to address growing public concerns about privacy in the United States and Europe, in particular.

Scholarly examinations of individual privacy are rich and varied. Some researchers tackle the implications of concerns about its erosion, while others assemble arguments for its abandonment, and still others put forward well-reasoned cases that privacy rights require public policy support. Interestingly though, privacy is still not well-defined in American culture, and there remain differing views on exactly what deserves privacy protection, if anything.

Viewed from other shores, privacy takes on even more variety, as a result of differing social norms about acceptable behaviors, and what kinds of activities and information should be under the control of every individual.

In other words, the forces that cyber philosopher Lawrence Lessig laid out in the 1990s as the foundations of the constraints we apply in today’s online world – law, social norms, the marketplace, and code, referring to the computer languages that have built the Internet and its myriad applications – all of these forces are engaged in determining what kind of Internet culture we will experience in the years to come.

The question is what privacy values will this Internet culture share? Will these values be dictated by market forces racing to profit from Web 2.0 uses?
Will the privacy we value in the future adopt “radical transparency,” the notion that drove the founder of Facebook, Mark Zuckerberg, to turn his dorm dream for how to meet girls into a global enterprise worth billions of dollars? What is lost if privacy is no longer there?

Or will U.S. policies on control and access to information online move more in the direction of the policies that apply in European Union nations, where the right to personal privacy is enshrined as a fundamental human right?

This examination considers whether radical transparency would be a social norm that is consistent with the ethical principles that have supported Americans’ ideas of individual freedoms and privacy in the past, or whether a new approach that achieves greater balance among these social goods is possible. Following this analysis, several approaches for consideration by U.S. policymakers to establish a greater equilibrium between the desirable, but competing rights of freedom and privacy, will be discussed.
CHAPTER ONE

LEGAL AND POLICY PERSPECTIVES ON PRIVACY IN AMERICA

That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.1

— Samuel Warren and Louis Brandeis, “The Right to Privacy”

Warren and Brandeis wrote those words 122 years ago, but the opening lines of their law review argument for Americans’ right to privacy could just as easily have been written yesterday.

The “demands of society” have never stopped evolving as the industrial era gave way to the information era and the appearance of more advanced technologies to enable activities by citizens that would have been science fiction speculations when the two law partners in Boston wrote this seminal essay in the *Harvard Law Review*. In 1890, the new technology on the American scene that spurred them to argue for refreshing the legal principle of the “right to be let alone”2 was the growing popularity of a camera of sufficiently lighter weight and size to be portable, and ultimately, to support what became known as ‘spot news’ photography. “Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life,”3 Warren and Brandeis complained in launching their case for the broader principles at stake involving privacy.

Today, it is information and digital technologies that have given rise to fresh concerns about where to draw the lines among the right to be let alone and other social
goods such as law enforcement and national security protections, and other rights, including freedom of speech, press freedom, and even free market competition. In 2012, the majority of Americans rely on digital communications for everyday business, government, and social interactions. Thanks to the Internet, the digital realm is now central to the debate about a growing list of important questions, including: Are we entitled to control our personal information in online commerce? Does anyone have the right to profit from our personal digital information if we freely post it on a social media website? If we put personal information in an email, or enter personal data on a social media website like Facebook, is that information freely available for any other purpose? Who owns citizens’ personal information when it is collected and shared as part of vast databases? Does the full protection that Warren and Brandeis spoke of still apply, or is society advancing toward a new social norm – perhaps even a new framework for evaluating privacy – one that gives greater weight to freedom of speech, transparency or the radical transparency concept labeled and espoused by Facebook founder Mark Zuckerberg? And perhaps most important, is the privacy debate in the twenty-first century about where to draw the lines among sometimes competing individual liberties, or are there overarching societal interests that should define where the privacy lines are drawn?

Answers to these questions are anything but straightforward, as the nature of privacy is complex, containing many facets depending on the particular aspect of privacy being examined. It is certainly true that privacy issues attract many special interests with ample arguments. Before beginning the examination of whether Facebook’s radical
transparency is a suitable normative view of privacy, it is helpful to focus on what constitutes privacy in contemporary legal and policy terms. Leading information policy and cyberlaw scholar Daniel Solove has developed a helpful taxonomy around which he groups four principal sets of activities that encompass modern privacy and concerns about how, when or if, it is protected: information collection, information processing, information dissemination, and invasion.⁴

These four categories will help in considering answers to the questions posed here, as each of the four activities play a part in what Facebook represents in the information age. As the world’s leading social media site, Facebook enables the collection of vast amounts of personal information about its users. Facebook also processes information in various ways, and disseminates information to others, including application developers, advertisers, and consumer data aggregators, in order to make a profit. Finally, according to privacy advocates who have taken Facebook to court, it is accused of having deceived its users and invaded their privacy. It is no surprise, then, that many of the proposals to strengthen U.S. privacy laws have social media and its applications at their center.

Chapter One presents a brief legal and policy overview about privacy that forms the background to this examination of the questions of where privacy is headed in American society now that Facebook is the dominant social media platform. As the famous brief by Warren and Brandeis exemplifies, a central thread running through the history of privacy is technological change; as technology has evolved, so has the need to reexamine the privacy implications for society and its citizens.
Technology’s Impact on Privacy Law and Policy

As Warren and Brandeis noted more than a century ago when portable cameras came into wide use by the news media, Americans had been accustomed to the presumption of the privacy of their personhoods and their property since the founding of the country. In their homes, Americans enjoyed privacy behind walls and locked doors and curtained windows from prying eyes and ears. In addition, “the principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.”\(^5\) This expression of “inviolate personality” has been generally interpreted as an assertion of the individual’s right to autonomy, and the principle of privacy as attached to personhood as well as property.

Individual autonomy, in their view, had started out in earlier times as a remedy of law for “physical interference with life and property,” and over time, as “there came a recognition of man’s spiritual nature, of his feelings and his intellect,” the law asserted broader rights for the individual, including “the right to enjoy life – the right to be let alone.” Warren and Brandeis argued that “the right to liberty secures the exercise of extensive civil privileges; and the term ‘property’ has grown to comprise every form of possession – intangible, as well as tangible.”\(^6\)

According to Solove’s contemporary legal analysis, Warren and Brandeis traced society’s evolving understanding of individual ‘harms’ to privacy into extensions of legal recognition, including laws against nuisance for such nonphysical injury as offensive noise, odor, dust, and smoke; laws protecting intellectual property; and even advanced
the case for privacy protection in the tort law against harms that result in “injury to the feelings.” In so doing, their precedent-setting legal analysis links changes in technology and society’s changing perceptions of norms and values with consequent legal actions, followed by changes in legislation to support privacy protections. The Warren and Brandeis analysis illustrates the role of technology as a catalyst in prompting changes in how privacy is understood by society.

Technology is the omnipresent game-changer in contemporary discussions about privacy, although Priscilla Regan, in her comprehensive look at U.S. privacy law, wryly observes that the degree to which the rise of digital technology has affected how society perceives privacy is a something of chicken-or-egg debate. “Before telegraph, telephone, and electronic mail, it was possible to listen in on or overhear the personal conversations of others,” she notes in a contextual introduction of three schools of thought on the impact of technology on social change: the technology determinists, neutralists, and realists.8

The technology determinists, in Regan’s view, believe technology has become the single most important source of change in modern society, independent of social change itself, which they view as dependent on advancing technology. Those who espouse this view tend to equate technology with negative influences, as a dehumanizing force. Next are the technology neutralists, who reject the idea of technology as independent of people, but see it as a tool that can be shaped to human desires and needs. Finally, there are the technology realists, she says, who occupy “the middle ground in this debate.”
Realists see technological developments as a mixed blessing of opportunities and problems.  

“Technology realists adopt a more complicated view of privacy and technology,” Regan writes. “They see technology as an agent of change and believe the actual direction of change depends on both the capabilities of the technology and the uses to which it is put.” In other words, the realist sees neither technology nor society as the driver, and she implies there is also the possibility of unintended consequences acting on society over time, as not all uses of a particular technology are readily apparent.  

Most important, Regan states categorically (no doubt based on an exhaustive examination of the transcripts of hearings and public deliberations on privacy legislation from the 1960s through the 1980s) that “the role of public policy is largely reactive – technological changes are adopted, anticipated or unanticipated consequences occur, and those dissatisfied with the consequences press for change.” It is also worth adding, as it will return later in this analysis, that Regan concludes it is difficult to reverse the public policy course once it is initially set “not only because the technology itself pushes in a certain direction but also because powerful social, economic, and political actors may benefit from that course.”

**The Judicial Legacy of Privacy**

In her analysis of U.S. privacy law, Regan divides the history of legislation that began in the 1960s into three categories of privacy concerns – information privacy, communication privacy, and psychological privacy, in order of the amount of legislation devoted to each type. Information privacy issues are concerned with use of personal
information collected by organizations from the government to banks, credit card companies, education institutions, and so forth. Communications privacy in the period from the 1960s through 1990 dealt with interception of discussions between two parties, whether printed, verbal or electronic. And psychological privacy involved questions about probing individuals’ thoughts and attitudes, principally through the use of polygraph testing.

Since 1990, however, more attention has been focused on the privacy, or lack thereof, in transactions between individuals and the private sector, as the early wave of privacy legislation was devoted to laying the groundwork for the relationship between the individual and government by requiring more government transparency while securing individuals’ personal information. The public discussions about privacy, outside legal briefs and tort actions, have been anything but clarifying.

In America, privacy seems to have always been a complex, and somewhat murky concept. Many legal scholars in this field, along with philosophers and social scientists who have examined privacy in modern America, make a point of observing, as Regan and Solove both do, that the word privacy does not appear in the U.S. Constitution or the Bill of Rights. However, as Helen Nissenbaum explains, in a seminal review of privacy in the context of society and technology, privacy protection is embodied in a number of Constitutional amendments, including: the First, assuring freedoms of speech, religion, and association; Third, protection against being coerced by government into quartering soldiers in private homes; Fourth, assurance against unreasonable searches and seizures;
Fifth, protection against self-incrimination; Ninth, a guarantee of general liberties; and the later Fourteenth, protection of personal liberties against actions by states.\(^{13}\)

Given that Warren and Brandeis connected privacy’s common law roots with its Constitutional foundation, the Constitution has served ever since in U.S. courts as the bedrock legal framework for cases involving privacy, including the recognition that these amendments reference privacy protections as part of citizens’ rights, notably the right to be left alone.\(^{14}\) And perhaps based on this inherent right given voice by Warren and Brandeis, many Americans still assume their privacy is somehow protected when they go online to chat or order a video to watch at home.

Warren and Brandeis are considered the founding thinkers of the legal framework for privacy as American society began experiencing rapid technological changes. Regan, Nussbaum, Solove, and other researchers agree that Warren and Brandeis have that distinction, and that perhaps second in influence is William Prosser, who argued in a 1960 *California Law Review* article on privacy, that there are four types of torts arising from privacy invasion – intrusion, disclosure, false light, and appropriation.\(^{15}\)

Solove explains that Prosser’s great contribution “was to synthesize the cases that emerged from Warren and Brandeis’ famous law review article.” However, Solove also notes that Prosser was only concerned with tort law, which fails to protect an individual prior to injury, and that Prosser was writing nearly a half-century before the information age made the exposure (even unwitting) of private information so easy.\(^{16}\)

Indeed, astonishing change has taken place since the 1960s, when Regan reports that by the middle of that decade “concerns about privacy and technology were reflected
in a ‘literature of alarm’ that was instrumental in placing the issues of information
privacy, communication privacy, and psychological privacy on the policy agenda.”17

In fact, she finds that from the time of Warren and Brandeis’ writing, privacy was
“not again a major topic of philosophical interest in the United States,” until the 1960s
when legal interest was sparked in light of technological changes that appeared to
threaten privacy.18 Public interest was aroused when it became widely known that
government agencies were making increasing use of computerized databases for
statistical and other administrative purposes with little or no safeguards in place for the
protection of citizens’ private information.19 Of special concern to the media and
Congress was a proposal put forward in 1965 by the Social Science Research Council to
create a federal data center, in effect, a central repository to manage uses of personal
information held by government entities. As Regan chronicles, this proposal resulted in
much public deliberation and ultimately led to the passage of the Privacy Act of 1974.20

This landmark law established the principles for government control and access to
citizens’ personal information. It was passed after years of intense advocacy efforts over
the need to legally shield citizens from the increasing intrusive power of federal
government over personal, even intimate, information about citizens,21 as once-paper
records about individuals were being turned into vast computer databases containing
private and personal information, from military records to census, financial, health, and
law enforcement records.

However, there were doubts about whether the law was sufficient, and President
Jimmy Carter appointed members to a U.S. Privacy Protection Study Commission soon
after its passage to examine the issues more broadly. After numerous hearings and meetings over a two-year period, the Commission reported its findings to Carter, recommending a broader national policy to more fairly guide the way public and private sector entities keep the records of individuals.  

Looking to the future, the Commission observed that the precarious balance between individual rights and the duties of the government deserved ongoing attention from policymakers:

The broad availability and low cost of computer and telecommunications technologies provides both the impetus and the means to perform new record-keeping functions. These functions can bring the individual substantial benefits, but there are also disadvantages for the individual. On one hand, they can give him easier access to services that make his life more comfortable or convenient. On the other, they also tempt others to demand, and make it easier for them to get access to, information about him for purposes he does not expect and would not agree to if he were asked.

This cost-to-benefit calculation of trading some privacy for some other convenience that was referenced by a commission during the Carter administration remains to this day a central issue in legal and policy discussions. As Solove concludes, even when policymakers and the courts recognize a problem with potential invasion of privacy, attempts at solution “can also falter in understanding its nature and effects.”

Solove finds that “on the surface, the [1974 Privacy] act embodies a pluralistic conception of privacy that recognizes many of the problems in the taxonomy, such as information collection, processing, and dissemination,” but fails “because its enforcement provisions do not adequately address the harms created by these problems.” The principal method of enforcement all too often since the mid-1970s has been a lawsuit filed by an individual against a federal agency after some loss of privacy in an attempt to
show a personal harm or injury flowing from mishandling or disclosure of their personal
information.

Also in 1974, Congress passed the Family Educational Rights and Privacy Act, to
protect the confidentiality of all student records, and impose certain standards for
accurate record-keeping on all schools that receive federal funds. It also included an
important provision contained in the Privacy Act that granted students and their parents
access to school records, and the opportunity to challenge contents on accuracy
grounds.\textsuperscript{26}

With these legislative efforts, Congress set out the principles that citizens as
consumers, students, members of the Armed Forces – in whatever role they encounter the
public sector – have the right of access to see records about them, and to challenge the
accuracy of the contents.

Some legislation had come before, notably the Fair Credit Reporting Act of 1970,
and was followed by the Right to Financial Privacy Act of 1978,\textsuperscript{27} as members of
Congress began erecting the legal framework for government regulation of the collection,
processing, and dissemination of personal information by government arms like the U.S.
Internal Revenue Service, as well as credit reporting agencies and financial institutions.\textsuperscript{28}

All of these protections, however, presume that individuals monitor and initiate action in
the event they learn of a breach of their privacy or some inaccuracy in a public record
that resulted in some personal harm.

This great wave of privacy legislation also does not mean that legal interpretations
of privacy are any clearer as a result. An example is perhaps the most notable attempt to
come to grips with the balance between Fourth Amendment rights and surveillance of citizens by government, the 1967 Supreme Court decision in Katz v. United States. In Katz, as legal scholar Jonathan Turley explains in a Washington Post commentary, “the court was dealing with decades of increasing surveillance under the ‘trespass doctrine,’ established in 1928, which allowed the government to conduct warrantless surveillance so long as it did not physically trespass on the property of a citizen.” He argues that Katz represents a landmark decision “which is celebrated as saving privacy in the United States,” because in it the high court “articulated the principle that ‘the Fourth Amendment protects people, not places.’ The decision reversed a long erosion of privacy protection and required greater use of warrants by the government.” Turley asserts that this protection is once more under siege with an ‘all-seeing’ array of closed-circuit TV cameras and GPS tracking devices.

Turley is among the legal experts now concerned that the latest Supreme Court decision to reinterpret Katz for the digital age, Jones v. United States (handed down in January 2012) has exposed a huge seam in privacy protections by failing to affirm that it attaches to the individual rather than the individual’s property, and equally important, lets stand the ‘third-party doctrine.’ This doctrine, which liberal legal scholars consider pernicious in light of routine social and commercial interactions over the Internet, states that once an individual shares personal information with a third party, any ‘reasonable expectation’ of privacy is forfeited.

In the Jones decision, Justice Sonia Sotomayor takes up these failings, noting in a separate, concurring opinion that Katz is overdue for rethinking. The ‘third-party
doctrine’ previously upheld by the Supreme Court is a test “ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks,” Sotomayor writes. 31 She goes on to say:

Perhaps, as Justice [Samuel] Alito notes, some people may find the ‘tradeoff’ of privacy for convenience ‘worthwhile,’ or come to accept this ‘diminution of privacy’ as ‘inevitable’ . . . and perhaps not. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy [emphasis added]. 32

Barry Friedman, New York University professor of law, sees danger to privacy in how the Fourth Amendment was interpreted by the high court in the Jones decision. In a commentary in The New York Times, Friedman concludes the Court’s decision to outlaw warrantless search by GPS tracking was based on trespass of personal property, in this case, the criminal suspect’s vehicle, rather than the victim’s personal privacy. 33

In Friedman’s view, this property-focused argument “may turn the Fourth Amendment into a ticking time bomb, set to self-destruct – and soon – in the face of rapidly emerging technology. Dog sniffs. Heat sensors. Helicopter flyovers. Are these ‘searches’ in within the meaning of the Fourth Amendment?” He argues that the most important legal principle to redefine for modern times is the ‘reasonable expectation’ of personal privacy in an age of omnipresent technologies that can track us wherever we go and record what we do. 34

Adding to the legal confusion is that U.S. law and legal interpretations have maintained the responsibility with the individual to ‘police’ his or her records to ensure that personal information is accurate and secured within the boundaries of the law. The reliance on individual responsibility, combined with the ‘third-party doctrine,’ has been
enshrined in a *laissez-faire* approach to privacy policymaking involving the private sector.

With the widespread adoption of cyber-harvesting of personal data by for-profit enterprises, access to personal data by private-sector entities has become an increasing focus of public debate since the early 1990s. The ongoing discussion also has drawn more and more special interests on all sides of the debate, including privacy and consumer advocates pressing for stronger protections from inappropriate access to citizens’ private information, while commercial interests appeal to lawmakers to take actions that will benefit their competitive position in the marketplace. Meanwhile, the federal government — which has an overriding interest in protecting citizens’ privacy online — remains largely silent.

**Privacy Policy Since 2000**

By the early 2000s, online interactions became a focus of interest in policy debates around privacy. Surrounding these public discussions is a rich body of scholarship concerned with privacy from every perspective — the philosophical and ethical to society and the law. Some researchers build arguments against the unintended, long-term societal consequences of the erosion of privacy, while others assemble arguments in favor of a diminished ‘reasonableness expectation’ of privacy in an era of increasing transparency and peoples’ willingness to exchange personal information in return for other benefits, and still others put forward well-reasoned cases that privacy rights in the digital age require novel approaches to public policy support. Interestingly though, digital privacy is still not well understood across American society, and views
about what deserves protection appear to be divided in 2012 as the Internet has expanded its reach into every aspect of life.

Solove, a leading thinker in cyberlaw and information policy, began his eminent review of U.S. privacy law by calling privacy “a concept in disarray.” As Solove concludes after more than a decade of work in the field, it is “a sweeping concept, encompassing (among other things) freedom of thought, control over one’s body, solitude in one’s home, control over personal information, freedom from surveillance, protection of one’s reputation, and protection from searches and interrogations.”

Viewed from European shores, privacy takes on even more variety, as a result of other cultures’ differing social norms about what behaviors, activities, and information should be kept private or protected as private. In other words, the forces that cyber philosopher Lawrence Lessig first laid out in the 1990s to govern over the values we apply in the online world – law, social norms, the marketplace, and the architecture (code) that is used to create the Internet and its myriad applications – are still being applied inconsistently and sometimes in contradictory ways in determining not only what kind of Internet culture we currently live in, but also the values that will inform this experience in the years to come.

Currently, at least 26 U.S. public laws, and numerous state statutes, govern topics connected to access and control of personal information that can apply in cyberspace. Primarily, these laws are aimed at establishing control, maintenance, and security standards for government agencies that have statutory obligations to gather personal information about citizens, and to set up rules governing how such ‘controlled’ data
might be made accessible to other government agencies. At the state level, statutes focus much attention on requiring that organizations must adhere to privacy policies and make them available to consumers whenever personal information is involved.

By 2010, digital privacy concerns began escalating as more cases of unintended consequences of life online have made headlines, and attracted greater consumer attention. What citizens once assumed to be a protected ‘reasonableness expectation,’ privacy is being widely described, once again, as under assault. Media coverage frequently describes cyber encroachments: how hapless individuals’ personal views have been exposed publicly, leading to humiliation and reputational harm, loss of employment, and in the case of some vulnerable individuals, suicides. In addition, there is the growing realization that many Americans have unwittingly traded their personal information in return for ‘free’ access to the features of popular social media like Facebook, resulting in a variety of unintended consequences of dubious value. To illustrate, here is a brief sampling of events involving Facebook that took place in 2011:

**In January:** A National Labor Relations Board judge was to consider whether a medical transportation company illegally fired a worker after she criticized her boss on Facebook – the first complaint to the federal agency linked to social media. This followed media coverage of a former high school teacher in Georgia who sued the school district in Barrow County after being forced to resign over Facebook photos that showed her holding a glass of wine during a European vacation.38

**In February:** An online dating site (lovely-faces.com) commandeered the personal information of 250,000 Facebook users and reproduced their names and photos along
with a link to their Facebook pages, and gave its users the option to ‘arrange a date’ with the unsuspecting Facebook users. Facebook promised ‘aggressive legal action’ against those who take advantage of its users who haven’t adjusted their security settings to block non-friends from seeing their posts and photos by doing what is called ‘scraping’ of profiles.39

In November: A widespread spam attack placed violent and pornographic photos on Facebook users’ profile pages. A Facebook spokesman explained that the affected accounts were being shut down, and that the users involved were “somehow tricked into copying and pasting malicious code into their browser bars,” which enabled hackers to access their profiles and post whatever they wanted on the Facebook pages.40

In December: Facebook released a revamped profile feature called Timeline that makes a user’s entire history of photos, links, posts, and other shared information accessible with a single click, in what site founder Zuckerberg referred to as “an important step to help tell the story of your life.” Critics immediately began protesting Facebook’s complex privacy settings that seemed designed to make the new feature difficult to ‘wall off’ from the world.41

Each of these events share common threads: unintended, even malignant, use by others of personal communications the Facebook user intended to be private and accessible only to their friends, and the lack of legal protection for the unwitting social media user.

In effect, personal privacy is anything but assured online in today’s world. It is in fact a murky business once citizens leave the realms of their domiciles, physical property,
and ordinary activities that are governed by settled common law or tort associations spelled out by Prosser, and enter the digital world of global business activity and commercial interactions, and especially voluntary social networking activities.

A principal reason, as Solove and Regan have observed, is that U.S. privacy law has continued to allow the marketplace, as determined by the private sector, to follow its own technology path and set its own standards, while providing a legal framework primarily aimed at protecting privacy of individuals’ increasingly transparent transactions with the public sector. The result has been a hodge-podge of private sector ‘privacy policies’ that frankly favor the business rather than the individual. As a result, Americans find themselves all too frequently having to read multiple screens of tiny, legalese online to figure out if they want to ‘opt out’ of some future use, or all too often, face a ‘take it or leave it’ blanket ‘accept’ in order to avail themselves of a particular online service or application. An editorial in The New York Times observed:

Considering how much information we entrust to the Internet every day, it is hard to believe there is no general law to protect people’s privacy online. Companies harvest data about people as they surf the Net, assemble it into detailed profiles and sell it to advertisers or others without ever asking permission.42

Yet despite growing public interest in the subject, privacy issues are maddeningly complicated for policymakers, and even for online businesses, because there are so many interests at stake. Not surprisingly, information and communications technologies have advanced at speeds that have left public policy far behind in trying to maintain basic privacy protections, just as Regan predicts.
The result is that attempts to legislate now involve the exceedingly difficult task of ‘walking back’ from commercial activities that the private sector has been free to exploit for more than two decades.

Early in 2012, the Obama administration attempted to set the tone for lawmakers in the 112th Congress interested in strengthening privacy protections by creating a task force that produced a “Consumer Privacy Bill of Rights.” In it, the White House task force sets out seven principles the president hopes to see frame U.S. policy:

**Transparency:** Consumers have a right to easily understandable information about privacy and security practices.

**Respect for Context:** Consumers have a right to expect that organizations will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.

**Security:** Consumers have a right to secure and responsible handling of personal data.

**Access and Accuracy:** Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data are inaccurate.

**Focused Collection:** Consumers have a right to reasonable limits on the personal data that companies collect and retain.

**Accountability:** Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.43

The White House initiative was followed by publication of a U.S. Federal Trade Commission study on protecting consumer privacy that includes a number of voluntary ‘best practices’ recommendations for businesses and policymakers in line with the “Consumer Privacy Bill of Rights.”44

The results so far have been mixed. Several of the major Internet companies with search engines (including Google, Microsoft, and Apple) have agreed to support a ‘do not track’ choice for consumers on their websites;45 but so far, despite no fewer than 19 bills
and one discussion draft circulating since the end of January 2012, the 112th Congress has taken no action on privacy legislation. Among the many bills introduced are measures that would add new protections in such areas as: children’s privacy online; standards for the collection, storage, and use of consumers’ personal information; standards for reporting data breaches and identity theft; and standards and tougher privacy provisions for geolocation surveillance.

One of the best-known of these bills aims to provide consumers with stronger protection against online tracking, known as the *Do-Not-Track Online Act* (S. 913), introduced by Sen. Jay Rockefeller (D-WV), chairman of the Senate Committee on Commerce, Science, and Transportation. If enacted, this legislation would direct the U.S. Federal Trade Commission (FTC) to develop regulations regarding the collection and use of personal information by tracking users’ online activities, and is reminiscent of the popular FTC program, the National Do Not Call Registry, that allowed consumers to enter their land line and mobile telephone numbers to a government list to ‘opt out’ of receiving telemarketing calls.

As Congress considers possible legislation, other government agencies continue to pursue enforcement of existing federal regulations. Internet giants Google and Facebook are being forced to defend – and in many instances alter – their privacy policies to address growing public concerns about privacy. In fact, in the past year both have entered into consent decrees with the FTC for abusing consumers’ privacy.46,47

In the settlement, Facebook admitted to unfair and deceptive privacy practices, and agreed to establish clear, easy to understand policies for its users to govern sharing of
personal information, and to refrain from making any retroactive changes to its privacy policies without notifying users beforehand so they can adjust their privacy settings in accord with their preferences. In a lengthy blog post following the agreement with the FTC, Zuckerberg acknowledges mistakes:

Facebook has always been committed to being transparent . . . and we have led the Internet in building tools to give people the ability to see and control what they share. But we can also always do better. I'm committed to making Facebook the leader in transparency and control around privacy.49

However, Zuckerberg’s reassurances and even the FTC’s enforcement action failed to satisfy the social media platform’s critics, notably the Electronic Privacy Information Center (EPIC), whose executive director Marc Rotenberg declared that settlements with individual companies are inadequate in comparison to a federal law to protect consumer privacy online. EPIC was a leader in the coalition of consumer groups that filed the FTC complaint against Facebook. In an interview with The New York Times, Rotenberg said of the FTC: “We hope they will establish a high bar for privacy protection. But we do not have in the United States a comprehensive privacy framework. There is always a risk other companies will come along and create new problems.” 50

As the U.S. policy record currently stands, advancing privacy protections for the digital age remains an unanswered challenge. The reasons are, like privacy itself, complicated by lack of public understanding, and agreement among powerful interest groups, about what form protection should take, and even what deserves protection.

The next chapter examines the philosophical and ethical perspectives about privacy that have helped to shape the normative views of privacy in America, including
those of the marketplace and among the architects of the Internet age, and how those views are evolving in the era of Facebook.
CHAPTER TWO
THE VALUES OF PRIVACY IN AMERICA

Foundational political goods are those without which a nation state fails to be good and just. Privacy, I maintain, is a foundational good in the liberal west, to which the United States and similar nations should have a substantive commitment, as they do to personal freedom, and race and gender equality. People should be taught to value others’ privacy and their own. Government will sometimes be entitled or even required to reinforce privacy practices.¹

—Anita L. Allen, Unpopular Privacy: What Must We Hide?

Allen, a leading philosopher and legal scholar in the fields of privacy and bioethics, minces no words in asserting the social value of privacy and calls upon policymakers to take action even when privacy’s uses are not always appreciated in a diverse America. Her articulation of the personal and larger social values that demand robust support for privacy in a technological age early in the twenty-first century mirror those of Warren and Brandeis when they wrote their famous brief about privacy in the waning years of the nineteenth century, and warrants careful consideration if America is to maintain the democratic principles and values its people have always held most dear.

In 2012 America, privacy still enjoys widespread support as an individual right, if the national survey data is to be believed, yet its practice remains a complex puzzle in the online space. At a practical level, when citizens go online for socializing or doing business, they must stay focused on their actions in order to preserve what little privacy they still have. They must monitor their Internet data histories (and remove ‘cookies’ that will track their actions on websites), conduct rapid-fire risk assessments about whether to share personal information online (especially with new websites), and digest 4,000-word privacy policies like Facebook’s to decide how to manage what information they share on
the world’s largest social media platform. The relatively uncomplicated view of privacy such as the intrinsic ‘right to be let alone’ that Warren and Brandeis described in 1890 seems worlds away from the concerns Allen and other privacy experts describe today.

Privacy is now increasingly transactional, often traded away willingly or unwittingly in exchange for the convenience of online shopping or the fun of connecting with friends and family on social media sites like Facebook. According to national surveys of Americans’ attitudes, many people seem surprised to learn that their privacy is missing where once it was presumed to exist. Polling data by the Pew Internet and American Life Project shows that Americans consistently place a high value on privacy, and interestingly, there are signs that younger people — those who have most enthusiastically embraced social media — may be growing more alert to what they share on social media.

Even more important, behavioral studies suggest that when privacy choices are presented in understandable ways in online situations, a majority of people (including students) will choose to protect their personal information.

Much of this privacy muddle emanates from the incredible speed with which computer and Internet technologies are advancing — a situation that philosopher James H. Moor describes with characteristic understatement: “The malleability of computers allows them to be used in novel and unexpected ways for which we frequently do not have formulated policies for controlling their use.”

Could it be that citizens are becoming more cognizant of the potential loss of their privacy online as they are exposed to reports about the unintended consequences that can
flow from use of social media? Or is it possible that with each new technology to connect us and make daily living easier, Americans are growing increasingly tolerant of greater degrees of exposure of their personal information and lives online?

This chapter provides a look at the moral and ethical foundations for the viewpoint that privacy online is a value worthy of broad support, the position that seems to occupy the most shelf space in the scholarly examinations of privacy in the digital age. Included will be descriptions of leading scholars’ arguments about the principles in support of the idea that both individual and societal benefits flow from preserving privacy in cyberspace.

In the broadest sense, the scholars and researchers who study the implications of the presence or absence of privacy, tend to emphasize one side or the other of the privacy divide: the majority who contend privacy is a value that should be preserved and perhaps strengthened or at least made clearer and more understandable from a policy perspective; and the minority who see greater social utility in creating a more open and transparent society, using the Internet as one of the principal places to plant the flag for the values of transparency.

**Normative Conceptions of Privacy**

A December 2011 article on the lead business page of *The New York Times* is among many in recent years to describe the unfortunate to bizarre consequences of social media sharing:

Tyson Balcomb quit Facebook after a chance encounter on an elevator. He found himself standing next to a woman he had never met – yet through Facebook he knew what her older brother looked like, that she was from a tiny island off the coast of Washington and that she had recently visited the Space Needle in Seattle.
“I knew all these things about her, but I’d never even talked to her,” said Mr. Balcomb, a pre-med student in Oregon who had some real-life friends in common with the woman. “At that point I thought, maybe this is a little unhealthy.”

As this article was published, Facebook boasted more than 800 million active users globally, with approximately 200 million in the United States, or roughly two-thirds of the U.S. population. In this same period, Facebook launched a new feature called Timeline, a rolling profile that makes every user’s entire history of photos, links, comments and other exchanges, accessible with a single click. Founder Zuckerberg told a Web developer conference shortly before it went live: “We think it’s an important next step to help tell the story of your life.” While it may be true that the Timeline serves as a virtual scrapbook with settings that allow users to edit, hide or display items, Facebook skeptics are concerned about its practical effects.

Nicole B. Ellison, a professor of information studies at Michigan State University and researcher into Americans’ online behavior, observes that applying this feature retroactively five years after the site opened to the general public places a large burden on Facebook users. But just as important, Ellison says, this extra degree of permanent exposure adds a complication with unknown consequences. “What does it mean to reinvent yourself after high school, after college? Or will people completely go back and edit their histories? And how will that shape the way we view ourselves and our friends?” In other words, how will such behaviors affect social norms of truthfulness, among other moral principles? Or, in the case of the pre-med student, what social norms led him to conclude that Facebook presents him with an unhealthy version of what his generation refers to as ‘TMI, too much information’?
These are among the many examples of unintended ethical consequences that can occur when people use social media like Facebook. Nissenbaum, the preeminent scholar on law, privacy, and technology, describes at least three basic types of privacy issues that arise in the social media context: individuals posting information about *themselves* that later causes problems; posting information about *others* that leads to unintended troubles for one or both parties; and finally, the impacts of the monitoring and tracking of social media interactions by sites like Facebook in order to make money on users’ information.\(^6\)

The student appears to have responded to personal information about others that somehow crossed the social boundary of what he believes is appropriate to know about a complete stranger.

What ethical theories or touchpoints do people like Tyson Balcomb apply who value privacy and are considering some issue or question relative to sharing personal information online?

Nissenbaum’s comprehensive analysis of the legal, ethical, and social aspects of the privacy landscape provides an excellent framework for reviewing the theories of privacy currently being applied in scholarly discussions. She divides contemporary analyses into three groups of theories: normative as distinguished from descriptive accounts; normative approaches that frame privacy in terms of either access or control; and finally normative descriptions that focus on whether privacy should be defined in terms of its social goods or private values.\(^7\)

In this section, an overview of each pair of approaches is considered, beginning with the descriptive-normative views.
A descriptive account of privacy is essentially values-neutral, in that it states what privacy is without asserting that it is a good that should be retained and protected. As philosopher Ruth Gavison explains, a descriptive account of privacy simply lays out the degree of access others have to any individual through information, attention, and physical proximity. But she carefully distinguishes between what she terms the concept of privacy, which “should be neutral and descriptive only, so as not to preempt questions we might want to ask about such losses [of privacy],” and discussions of the benefits or harms resulting from the actual experience of privacy’s presence or loss. She goes on to explain that the descriptive concept of privacy does not eliminate the fact that privacy has value. 8

While acknowledging the utility of a neutral statement of facts about privacy in defining its framework in given situations, Nissenbaum nevertheless asserts that “most experts are drawn solely to issues surrounding privacy’s normative significance and simply finesse the question of whether a neutral concept is either plausible or needed.”9

Indeed, as Dean of the Yale Law School, Robert C. Post states in a discussion of privacy’s social foundations, there is no compelling reason to discuss privacy in a purely descriptive way, as any discussion of degrees of privacy — its presence or absence — constitutes a de facto judgment that normative value is part of its core meaning:

Whatever the virtue of such neutral definitions of privacy, they are most certainly not at the foundation of the common law, which rests instead upon a concept of privacy that is inherently normative. The privacy protected by the common law tort cannot be reduced to objective facts like spatial distance or information or observability; it can only be understood by reference to norms of behavior.10
The normative framework for describing privacy delves into what specific values, or categories of values, privacy affords. The second grouping Nissenbaum describes divides normative discussions into those focused on privacy as a matter of access, and those that argue privacy is derived from control over the type of privacy in question, whether it be physical, informational, or proprietary, as Allen writes.\textsuperscript{11}

Allen blends elements of access and control in her policy-focused analysis of privacy by setting out three spheres for privacy: physical, informational, and proprietary. She calls these the “everyday meanings of privacy.” Each of these she defines in terms of access to the individual, with elements of loss of personal control. Physical or spatial privacy “is disturbed when a person’s efforts to seclude or conceal himself or herself are frustrated.” Informational privacy is disrupted “when data, facts, or conversations that a person wishes to keep secret or anonymize are nonetheless acquired or disclosed.” Allen lists locational or geographic privacy as a subset of this. Finally, “we can also speak of ‘decisional,’ ‘proprietary,’ ‘associational,’ and ‘intellectual’ privacy,” she writes.\textsuperscript{12}

Philosopher Jeffrey Reiman offers a succinct and similar way of bringing together the two facets of the normative values associated with privacy when he defines privacy as “the condition [control mechanism] under which other people are deprived of access to either some information about you or some experience of you.”\textsuperscript{13}

Whether access or control, Nissenbaum concludes that “although a scan of literature, court records, and media reports reveals that most of what is written about privacy assumes it to be a form of control, accounts in terms of access have tended to be more precise and conceptually better developed.”\textsuperscript{14} Even so, she notes that in everyday
sense, the value most citizens place on access and control work in tandem “to capture essential aspects of privacy that we seem to care about.” In other words, most people assume control over personal information is an important privacy dimension, but so is the degree of access others have to this information, regardless of who is in control.

Scholars strive for clarity and precision in descriptions of privacy in part because every right reserved for individuals imposes certain responsibilities on all individuals and also on society’s institutions. For example, the right to free speech means that everyone is obliged to tolerate that speech, even if it is bigoted, or inflammatory, or otherwise at odds with society’s norms. Similarly, when citizens have a right to privacy of their information online, governments at all levels as well as private sector businesses that operate websites or social media portals, for example, have the responsibility of ensuring that right is appropriately supported.

Nissenbaum’s final set of categories around which experts discuss privacy’s normative values focuses on social goods or private goods. Starting with privacy’s normative value to the individual, a number of scholars, including Nissenbaum, Gavison, and Allen, argue that privacy supports a variety of important characteristics for human flourishing, including: well-being, creativity, freedom, and personal autonomy.

In their view, because people do not always act in ways that are consistent with their own or society’s best intentions, privacy is a necessary condition for individuals to flourish in a free society; in other words, to be free to develop as people, and to find their own creative, intellectual, and spiritual paths, free from prying eyes or undue outside influences.
Moral autonomy occupies a central place in discussions about the need for privacy protections in the view of many scholars. Privacy is seen as a form of personal autonomy in that it is intrinsically bound to the ability of an individual to be self-governing, acting on principles that are his or her own and not assimilated unexamined from society at large. Like autonomy, privacy allows for “self-determination with respect to information about oneself,” as Nissenbaum explains.\(^{17}\)

Philosopher Jeroen van den Hoven argues that the absence of privacy in modern society is a serious encroachment on human autonomy:

\[
\ldots [T]his\,\text{ conception of the person as being morally autonomous, as being the author and experimenter of his or her own moral career, provides a justification for protecting his personal data. Data-protection laws thus provide protection against the fixation of one’s moral identity by others than one’s self and have the symbolic utility of conveying to citizens that they are morally autonomous.}\(^ {18}\)
\]

Reiman argues that the normative value of privacy to the individual lies in its ability to ensure: “the protection of freedom, moral personality, and a rich and critical inner life.”\(^ {19}\) In a well-reasoned symposium essay, he writes that laws and social norms like those that support privacy are as follows:

\[
\ldots [D]esigned\,\text{ for the real people that they will govern, not for some ideal people that we would like to see or be. Just as Madison [James Madison in the Federalist paper No. 51] observed that if people were angels we wouldn’t need government at all, so we might add that if people were heroes we wouldn’t need privacy at all.}\(^ {20}\)
\]

Because people are not angels, Reiman adds, some of them will be inclined to punish their fellow citizens who act unconventionally, and then he goes one step further by saying that even if we assumed it was possible to somehow mold all citizens into people who could resist society’s pressures to conform, they would still require privacy in
order to learn how to develop their own views and achieve the confidence to express and live them.  

Interestingly, when privacy scholars are discussing the normative values of privacy to the individual, when taken in the context of a democratic society such as the United States, it is implicit that the moral good that results from individual privacy has concurrent value to the larger society as well.

**Privacy’s Value to Society**

In this regard, political scientist Regan offers perhaps the best summation of the normative value of privacy to both individuals and liberal democracies such as the United States, asserting that privacy is a collective value, a common value, and a public value.  

In Regan’s view, privacy is a public value in that it is constitutive of the rights a democracy holds most dear, including the rights of free (even anonymous) speech, and freedom of worship and association. By describing it as a “public value,” Regan relates privacy to any democratic political system as an “instrumental value”; i.e., “having value not as an end in itself but as a means of achieving other ends.” In order for the individual citizen to willingly and independently participate in the decision-making and operating of a free and open society, Regan asserts that citizens must be able “at some points [to] separate . . . from the pressures and conformities of collective life,” and cites Supreme Court decisions since the 1950s which have upheld privacy interests under the First Amendment and due process clause.  

As a common value, Regan argues that privacy preserves the core interests in these freedoms that all individuals in society share, whether or not they hold the same
beliefs or would take the same positions on public issues. “This is true not only for the traditional liberal interests in self-preservation and property but also for a host of other interests that people may define differently,” she writes, including those things individuals of free conscience believe, or what religious faith they practice, “all individuals have a common interest in this right.”

Collective value, Regan’s third concept that marks privacy’s importance to society, is “derived from the economists’ concept of collective or public goods, which are those goods defined as indivisible or nonexcludable; no one member of society can enjoy the benefit of a collective good without others also benefiting.” Regan maintains that like clean air or national defense, a collective good cannot be easily divided, nor can people be excluded from obtaining the benefit of a collective good once it is provided. Privacy, once rooted in society’s norms and laws, provides this same universal value.

Finally, no discussion of the values of privacy to society in the Internet era would be complete without reviewing the four constraints that govern activities in cyberspace, just as they do in ‘real’ space. Lessig, the visionary legal scholar, famously described how these four traditional values constraints – law, social norms, the market, and architecture – apply to behavior and activity on the Internet.

In Code, originally published in 1999, Lessig’s aim was to counter a then-popular notion that cyberspace could be neither controlled nor regulated. In it, he introduced a new and important idea, namely that the most important constraint in cyberspace, the analog to the natural and man-made ‘architecture’ of the real world, is the software and hardware code that allows cyberspace to operate. In this work and his updated
commentary in *Code: Version 2.0*, published in 2006, Lessig makes a compelling case that the code operating the Internet already regulates privacy protections (or lack thereof) online.\(^{27}\)

In effect, Lessig wanted citizens and policymakers to understand that the Internet is built in certain ways, that software and hardware is developed in certain ways, as a reflection of the influences of the other three constraints – what the law requires, what the marketplace wants in order to grow and be profitable, and finally, what social norms demand in the way of controls over, and access to, information online.

He summarizes the overarching issues posed by the four constraints this way:

The first generation of these architectures was built by a noncommercial sector – researchers and hackers, focused upon building a network. The second generation has been built by commerce. And the third, not yet off the drawing board, could well be the product of government. Which regulator do we prefer? Which regulators should be controlled? How does society exercise that control over entities that aim to control it?\(^{28}\)

The early Internet, as Lessig describes it, was designed for open access. Code, or architecture, since those early days in the 1980s and 1990s, has been increasingly influenced by the other three constraints on how the online world actually operates.

In Chapter One, a review of privacy’s legal and policy framework revealed a mixed result: much of individuals’ personal data is secured by federal legislation, but subject to overrides by law enforcement and other ‘national security’ interests. But in the online realm involving private sector entities, controls are scant and access to personal information has become a multi-billion dollar industry in just a few short years.

As Lessig observes, there are laws that provide some regulation in cyberspace, including copyright law, defamation law, and obscenity law (in addition to civil tort
remedies, of course). “How well law regulates, or how efficiently, is a different question.”

Considering the constraints of the marketplace on privacy, it is clear that the marketplace favors as much access to data — information about people — as possible, which leads to leaky privacy protections at best. “Data collection is the dominant activity of commercial websites,” Lessig notes. Even though his work does not take into account the market activities of social media sites like Facebook, there can be no doubt, especially now that the company has completed an initial public offering and is now a publicly traded stock, that Facebook is focused on extracting profits from its users’ information.

There is also little doubt about the effectiveness of the marketplace in driving the creation of hardware and software to support this type of commercial efficiency on the Internet; in other words, to make it easier for businesses to flourish online. This flourishing comes, in a certain sense, at the expense of every individual who logs on to the Internet and leaves a data trail of ‘cookies,’ marking every website they visit, and most likely, a digital record of transactions with online merchants, and at social media sites like Facebook. In the Internet age, personal information is just another commoditized product for sale.

The incredible wave of personal information has spawned an entirely new and burgeoning industry in data collection and analysis, and lies at the heart of the privacy concerns that still stalk Internet giants like Google and Facebook, as these companies look to profit from the wealth of information about people everywhere. Forrester
Research estimates that companies spend two billion dollars a year for personal data that results from this ever-growing trail of information.32

Facebook alone is responsible for staggering amounts of personal information about its users (like 750 million photos uploaded over a single weekend) but also for the extent of ‘face time’ it commands. “More than half of its users — and one of every 13 people on Earth is a Facebook user — log on every day,” reports Stephen Marche, a novelist who asks an intriguing question in an article in The Atlantic with the title, “Is Facebook Making Us Lonely?”33

Despite settlements with the FTC and elaborate privacy policy settings and preferences for its users, Facebook still manages to extract intimate details of its users’ lives for sale to advertisers and data aggregators. A Wall Street Journal examination of 100 of the most popular Facebook applications, or ‘apps,’ found some that seek email addresses, current locations, and sexual preferences of the app users and their Facebook friends.34

In fairness, app developers are required to ask people’s permission to access their Facebook data, and the site’s policies forbid app makers from using advertising companies unless they have signed agreements with Facebook prohibiting them from collecting personal information. But there are suggestions this control may not be adequate. The Wall Street Journal inquiry also found, according to data being collected by PrivacyChoice, a start-up that offers privacy services, that some apps are letting unapproved advertising firms track users.35 As a technologist who writes for Slate, Farhad Manjoo, puts it this way:
I don’t think most Facebook users have internalized how leaky the site can be. You should approach Facebook as cautiously as you would approach your open bedroom window. However restrictive your privacy controls, you should imagine that everything that you post on Facebook will be available for public consumption forever.\footnote{36}

In sum, it would appear that public law and the marketplace are not always effective in maintaining privacy — even as an option — in the online space.

This leads to the question of what effect do social norms about privacy have in governing any of the other three ethical drivers — law, marketplace or architecture?

**Social Norms About Privacy**

Recent surveys of Americans suggest that at least among adults ages 18 and up, concerns about privacy when using a social networking site have increased. Based upon polling conducted by the Pew Internet & American Life Project in April and May 2011, about two-thirds (63 percent) of Americans report having a profile on Facebook, and 58 percent of those say their profile is set to be private so that only friends can see it. Also of interest is that roughly two-thirds of these users also say they actively manage their profiles, which means they regularly review their page and sometimes delete comments others have placed there, delete their names from photos that were tagged to identify them, and even ‘unfriend’ people from their Facebook list of friends.\footnote{37}

In addition, privacy seems to be held in high esteem by young Americans. A Pew Internet & American Life Project Teen-Parent survey conducted between April and July 2011 confirms that social media use is widespread among young people ages 12-17 (76 percent), and that Facebook is the dominant choice (by 93 percent of those who use social media). Privacy appears to be of value to them, as 62 percent report relying on ‘friends-
only’ privacy settings, and more than half (55 percent) report they decided not to post something out of concern that it might reflect poorly on them in the future. 38

However, even if the social norm in the United States is the belief that privacy is important, there are signs that some Americans are coming to accept that in the absence of legal protections, the marketplace and code-writers of the Internet have already made information privacy all but impossible.

In an overview of the Pew Internet & American Life Project study, researcher Mary Madden wrote in 2012: “As social media use has become a mainstream activity, there has been an increasingly polarized public debate about whether or not ‘privacy’ can be dismissed as a relic in the information age.” 39

In Madden’s view, attitudes about privacy are increasingly aligned among those who take the ‘privacy-is-dead’ position based on the vast amounts of intimate details about their lives that Facebook users post, and interprets this to mean they have abandoned any ‘reasonable expectation of privacy,’ and those who believe that “the public still cares deeply about their privacy online,” but have been misled by the companies intent on making a profit with consumers’ personal information, and perhaps lack adequate information about how this information is stored and used. Still, she notes, social science research has “long noted a major disconnect in attitudes and practices around information privacy online. When asked, people say that privacy is important to them; when observed, people’s actions seem to suggest otherwise.” In other words, Americans may be somewhat hypocritical in what they say about privacy versus what they actually practice when they go online. 40
Madden’s introduction to the Pew Internet findings has zeroed in on one of the paradoxes of being human: What people report they do and value is not always how they actually behave and what that behavior says about their values.

As an illustration, a trio of university marketing researchers reported on two experiments that tested consumers’ intentions about privacy with their later actual behaviors, and found that a ‘privacy paradox’ does indeed exist: that is, consumers tend to report greater unwillingness to share personal information than they actually exhibit when presented with online marketing opportunities, whether from well-known (presumably more trustworthy) brands, or less-trustworthy merchants.41

In a *Journal of Consumer Affairs* report, the researchers said they designed their experiments as follows:

. . . [T]o investigate whether people say one thing (intend to limit disclosure) and then do another (actually provide personal details) during marketing exchanges. To that end, we report the results of two studies that demonstrate the existence of the privacy paradox and suggest that individuals’ considerations of risk and trust help explain why it occurs.42

Another group of researchers, from Carnegie Mellon University, conducted a behavioral study which examined the paradox from a different angle, looking into “whether the prominent display of privacy information will cause consumers to incorporate this information into their online purchasing decisions.”43

In a series of experiments reported on in 2007, the Carnegie Mellon research team confirmed what other studies from the early 2000s onward have found; namely, that few people make the effort to find — let alone try — to understand privacy policies on websites they are using. The Carnegie Mellon researchers acknowledge that the
dichotomies in stated concerns versus actual behaviors can have several causes, including: “incomplete information about privacy threats and defenses, to bounded ability to deal with their complex trade-offs; from low (and decreasing) privacy sensitivities, to behavioral phenomena, such as immediate gratification.”

Lessig implies a similar disconnect when he argues that informational privacy is worthy of preservation in the online realm, and that the most efficient way to accomplish it is to press for computer architecture to be designed to support a wider range of understandable and usable individual choices about privacy.

This can be done by creating privacy enhancing technology (PET) on the Internet, Lessig says. One of these PET technologies is a protocol called the Platform for Privacy Preferences, or P3P. This protocol would enable machine-readable expression of the privacy preferences of an individual as they go to specific sites on the Internet. The P3P function would automatically scan privacy policies of any website visited, compare those privacy settings with the individual’s pre-set preferences, and give an alert to conflicts or rate the site as secure for privacy.

Interestingly, the Carnegie Mellon research team found that if test subjects were given computers loaded with P3P-enabled Internet search tools designed to make it easier for them to understand privacy settings and evaluate the relative privacy risks of individual websites, they preferred privacy. About 60 percent of volunteers reported that privacy information influenced the sites they visited, and from which sites they would make purchases. Volunteer subjects were using computers that were connected to an Internet search engine called Privacy Finder, which was created at Carnegie Mellon.
University’s Usable Privacy and Security (CUPS) Laboratory to run P3P software. Privacy Finder connects to websites with P3P-readable privacy policies and displays them in everyday language.47

Social science experiments such as these, combined with the views of a number of privacy researchers, suggest that perhaps social norms about privacy in America may be changing—but to what view seems to be hard to say at present. Some norms, however, remain clear.

For example, a location-based social network that works with Facebook on smartphones, allows users to alert friends when they ‘check in’ with Foursquare. Meantime, another app for iPhone called “Girls Around Me,” uses publicly available information from Foursquare to enable men to locate women who are close by on a map, and also view their Facebook personal data and photos. When news of the ease with which strangers could potentially identify women in physical proximity to them, the public outrage was fierce and Foursquare was forced to quickly revoke access to its users’ locations.48

In a Wall Street Journal story discussing the Foursquare rebuke, Nissenbaum said the “Girls Around Me” app generated such a swift angry response because it violates a social norm against stalking women. “If social norms were fences,” she said, “any ethical, law-abiding person won't step over the fence.” In the absence of data-usage laws or norms, she said, “some tech companies feel unconstrained about using information in new ways that can seem creepy.”49
Disrespect for the boundaries of traditional social norms in the online social media space comes as no surprise to Jaron Lanier, the digital visionary and computer scientist who in 2010 wrote, *You Are Not a Gadget: A Manifesto*, in which he warned of the dangers of unintended consequences for society in some of the changes he sees resulting from Internet technologies. In a recent interview in *The New Yorker*, Lanier admits that social networking “has become difficult for the ordinary person to use with any security.”

In the *Manifesto*, Lanier writes eloquently of the dangers of Facebook and other social media sites, saying he knows a lot of young people who brag they have “thousands of friends on Facebook. Obviously, this statement can only be true if the idea of friendship is reduced.”

He then goes on to suppose, for the purpose of argument, that what he refers to as a ritualized accumulation of ‘friends’ on Facebook is not a reduction in what friendship actually means, but is still an end-state antithetical to the purpose of Facebook. “[O]ne must remember that the customers of social networks are not the members of those networks,” he explains as follows:

The real customer is the advertiser of the future, but this creature has yet to appear in any significant way as this is being written. The whole artifice, the whole idea of fake friendship, is just bait laid by the lords of the clouds to lure hypothetical advertisers – we might call them messianic advertisers – who would someday show up.

Lanier illustrates his point about the social intentions of social media by describing an ill-fated attempt Facebook made in 2007 to monetize its users’ information to potential advertisers with a feature it called Beacon. When Beacon was imposed on
users (apparently difficult to remove), it would broadcast any online purchase a Facebook user made to every person on that individual’s personal Facebook network. “But it meant that, for example, there was no longer a way to buy a surprise birthday present. The commercial lives of Facebook users were no longer their own,” he points out.54

The immediate outcry and revolt it inspired among Facebook users at the time, Lanier writes, “cheered me, and strengthened my sense that people are still able to steer the evolution of the net.” He concludes by observing that “the only hope for social networking sites from a business point of view is for a magic formula to appear in which some method of violating privacy and dignity becomes acceptable.”55

Despite Lanier’s eloquence, his is a somewhat lonely voice among the era’s best-known Digerati, most of whom are passionate about the values of transparency and openness on the Internet – with the notable exception of their preference for being able to remain anonymous in certain, if not most, Web interactions. This intriguing dichotomy will be part of the discussion in the next chapter, in its examination of the origins and values of transparency as a desirable normative value on the Internet and social media.

In addition to an overview of transparency’s history, the next chapter also will provide some examples of how openness in social media, Facebook in particular, has tremendous power, both positive and negative, for members of an increasingly global society.
CHAPTER THREE
FACEBOOK’S RADICAL TRANSPARENCY AS A SOCIAL NORM

The world moving towards more transparency could be the trend driving the most change over the next ten or twenty years. . . . But there’s still a big question about how that happens. When you ask people what they think about transparency, some get a negative picture in their mind — the vision of a surveillance world. Will the transparency be used to centralize power or to decentralize it? I’m convinced that the trend towards greater transparency is inevitable. But I honestly don’t know how this other piece plays out.¹

— David Kirkpatrick, The Facebook Effect

In The Facebook Effect, Zuckerberg talks at length to author Kirkpatrick about his conviction that the social media portal he launched “on a radical social premise — that an evitable enveloping transparency will overtake modern life,” “what at Facebook they call ‘radical transparency,’” will be a positive force for social good. But even Zuckerberg is concerned about who will ultimately control our information in this virtual world, and therefore define what privacy, if any, will be permitted.²

The founder of Facebook describes for Kirkpatrick two scenarios — one is Google, which indexes information by tracking and gathering data that its ‘web crawlers’ pick up on the World Wide Web and bring into its systems, or by sending around vans to photograph every street and building to add to its global map directories. “And the way they collect and build profiles on people to do advertising is by tracking where you go on the Web, through cookies with DoubleClick and AdSense. That’s how they build a profile about what you’re interested in . . . . But you can see that taken to a logical extreme that is a little scary.”³
The other scenario is Facebook, Zuckerberg explains:

… [W]e started the company saying there should be another way. If you allow people to share what they want and give them good tools to control what they’re sharing, you can get even more information shared. This is one of the most important problems for the next ten or twenty years. Given that the world is moving towards more sharing of information, making sure that it happens in a bottom-up way, with people inputting the information themselves and having control over how their information interacts with the system, as opposed to a centralized way, through it being tracked in some surveillance system. I think that’s critical for the world.4

As Kirkpatrick observes, it is comforting in a way to know that the architect of the world’s most popular social media platform is committed to protecting our ability to control access to our information. “But what guarantee could Facebook’s users possibly get that his good intentions will last indefinitely?” Kirkpatrick asks.5 Indeed.

Since this insider’s view of Facebook was published in 2010, Facebook has signed a sweeping consent decree with the U.S. government to atone for extensive privacy lapses, launched itself as a public company, and seen its stock valuation plunge to half of its initial public offering. Now, some tracking services are reporting that its user growth curve shows signs of stalling and perhaps reversing. There are rising concerns on Wall Street about Facebook’s ability to grow profits in the face of Nielsen and other independent media surveys showing declines in U.S. visitors to Facebook since November 2011.

Who is to say that Zuckerberg will retain controlling ownership of his company, or be in a position to defy investors who want Facebook to monetize more directly the world’s second largest information database about people — behind only Google itself?
More importantly, it must be remembered that even if Facebook does not permit Google to index its information (it does not as of this writing), Facebook the company will always be able to see all the information its users post there. Despite the passionate words of its founder and CEO, it also has a track record of disregard for its users’ personal privacy protections.

So where does this lead? If Facebook is the bellwether social media platform, blazing the trail that has us living more transparently online, does this mean Americans are embracing a new norm about sharing their personal information? If so, is this a desirable social good? What are the “perils and promise of transparency,” as one researcher puts it,\(^6\) translated from the macro scale of international diplomacy and nation-states’ relationships with citizens down to the micro level of interpersonal relationships amongst people in a society such as ours? Finally, and most importantly, what is lost if personal privacy online is no longer there?

Scholars and researchers who study the philosophical and moral foundations and ethical issues surrounding privacy tend to view the ability to control information about oneself in one of two ways: as a primary or secondary value within the hierarchy of essential social goods. Increasingly, it seems the argument that privacy is an essential value and a social good that contributes to the functioning of a democratic society is the dominant perspective. However, there are also a number of researchers who place greater emphasis on building a more open and transparent society, and argue that individual privacy is more appropriately a derived, or even secondary, social value.
For some of these scholars, the Internet is considered essential in advancing the cause of transparency among governments, and governments’ interactions with citizens. Several cite the benefits of social media by activists around the world to spread information and win more support in struggles against repressive governments as a positive development in the transparency movement. As a result, these scholars place transparency in a position of primacy among shared values of the early twenty-first century.

This chapter outlines some of these views in framing the case for the values of transparency, beginning with its philosophical foundations, and discusses the positions of adherents over time. The review will include the symbolic ‘all-seeing’ idea of a utilitarian reformer in the early 1900s, and a philosopher’s call in the mid-1940s for openness as the antidote to wars and genocides wrought by brutally oppressive and secretive governments.

Transparency’s contemporary adherents make compelling arguments that public and personal values, often arrayed in pairs of opposites like privacy or secrecy and transparency or openness, need to coexist in some form of balance. This case is the basis for scholars Burkart Holzner’s and Leslie Holzner’s sweeping look at the history of transparency as a harbinger of beneficial changes to societies over time, while Ann Florini views transparency as a key ingredient in her call for more reliance on transnational governance to solve the world’s toughest problems. Although Kristin M. Lord catalogs many of these same benefits from the transparency facilitated by the ‘information revolution,’ she cautions that rosy predictions that it will bring more peace
and democracy are misguided. Transparency advocate David Brin, scientist and author, offers a tit-for-tat solution by proposing ‘reciprocal transparency,’ which basically would create a system in which every citizen is empowered to ‘watch the watchers’ in order to maintain balance.

Based on this historical and contemporary context, Facebook will be discussed as a case study, looking at how the ideas it espouses have been received by users, and the consequences which have resulted, good, bad, and unintended, and what radical transparency could mean for individuals in the digital age.

Foundations of Transparency

First, transparency needs to be defined in the context of a discussion about ethics and public policy. In one obvious sense, transparency is the opposite of secrecy or privacy on the spectrum of values-laden descriptions of behavior, whether the term is applied to the ways of government institutions or individual human beings. A secret is the deliberate withholding of information that is desired, or potentially desired, by others. Privacy in the context of the information age is the degree of control individuals have over the uses and sharing of their personal information, and the access others are granted to that information.

Transparency is the openness among governments, societies, and individuals necessary to establish trust among strangers and across cultural boundaries. In the context of a Facebook user, it will be shown that a radically transparent person is exceedingly open; someone whose feelings and actions are expressed freely and are publicly available, even to their personal detriment or that of others.
In their historical analysis of cultural transparency, the Holzners explain that opacity, the social condition of having no available information, and secrecy are among the oldest conditions of statecraft, “ancient tools of authority in most, if not all, societies.”

The Holzners are among the scholars who note that there have always been pioneers calling for greater transparency as part of making authority more accessible, and therefore accountable, in a society. Brin observes in his eclectic examination of transparency that from the days of classical Athens, birthplace of democracy, only Pericles was calling for what we would recognize today as an “open society, where [all] citizens are equal before the law and where influence is apportioned ‘not as a matter of privilege, but as a reward for merit; and poverty is not a bar. . . .’” Plato and his allies had no use for such openness, he concludes.

Pericles and his supporters were derided and their ideas were discredited for centuries. Until Enlightenment thinkers in the eighteenth century rediscovered the history of the Athenian golden age, the idea of an open, democratic society was viewed as an aberration, Brin observes.

As the century of Enlightenment gave way to the nineteenth century’s mix of social reformers and pragmatists, English philosopher Jeremy Bentham gave form to his ideas for social and legal improvements in a novel design for prisons that would keep the inmates under control with what he described as “all-seeing” efficiency. Bentham’s Panopticon, which he promoted as part of his quest for establishing a humane legal system, consisted of a circular tower, with prison cells arrayed around the outer
perimeter and walled off from each other, and in the center, a shuttered observation deck for prison guards. This would make it possible to watch the inmates without them knowing when they were being watched, thus leading the inmates to compliant behavior with maximum efficiency.\textsuperscript{12}

Bentham was a reformer who advocated a broad pallet of individual and economic freedoms as part of his advancement of the “Greatest Happiness Principle,” associated with utilitarianism.\textsuperscript{13} His Panopticon design was intended to make prisoners “not only suspect, but be assured, that whatever they do is known, even though that should not be the case.”\textsuperscript{14}

Florini describes in her examination of the benefits of transparency in the twenty-first century, that Bentham’s Panopticon — though rather ignored in his own time — has proved to be a metaphor “irresistible to a host of social theorists, beginning with Michel Foucault, who in \textit{Discipline and Punish: The Birth of a Prison}, published in 1979, “seized on the Panopticon as a symbol of the nature of modern society, in which people are controlled by being isolated from one another and being made to believe they are being watched.”\textsuperscript{15}

Since then, Bentham’s Panopticon has been a negative icon for privacy advocates because, as Florini notes, “the technologies of the information revolution have rendered the Panopticon a plausible metaphor for daily life” that citizens need to guard against.\textsuperscript{16}

Communications scholar Oscar Gandy couched his concerns about where erosions to privacy are taking society by titling a 1993 book, \textit{The Panoptic Sort}; Reiman, the philosopher and privacy scholar, coined the term “informational panopticon” in
proposing a thought experiment to prove the social value of privacy asking people to imagine themselves living absent of any privacy in an informational fishbowl. The result was self-editing that quickly led to a behavioral spectrum from bland conformity to ready condemnation of individualistic expression. Reiman later penned, “Driving to the Panopticon,” a law journal article in which he frames the philosophical principles undergirding the privacy risks from the emerging highway technology that would apply ‘all-seeing’ tracking capabilities to the location of every vehicle on the road.

If extremes of transparency, like radical transparency, are akin to Bentham’s Panopticon, then it must be said that until quite recent times, such openness was not technologically feasible, and as a result, was not much discussed. On the other hand, extremes of opacity and secrecy were the standards for governance among nation-states, and personal privacy (if it was available at all) was bounded in the common law principle Warren and Brandeis expressed as the “right to be let alone.” This was small comfort to the millions of people caught up in twentieth century world wars and the horrors visited around the world.

As the war against Hitler raged, philosopher Karl Popper wrote *The Open Society and Its Enemies*, a two-volume reappraisal of the philosophy of Plato, followed by a similar analysis of Georg Wilhelm Friedrich Hegel, in which he made the case that their influence denied empiricism and thwarted the rise of human freedoms and democracy. In effect, Popper argued that the ideas of Plato and Hegel contributed to continuation of generations of despotic rulers and totalitarian governments, including Nazism and Marxism.
Popper’s work today is considered important in turning the intellectual tide against the philosophy and ideals of communist totalitarianism. As the Holznens write: “Popper’s work was a clean break with much of earlier historical philosophy: Plato, Hegel, Marx, all were enemies of the open society.” Popper cites the call in Pericles’ famous funeral oration, in which he declares, “We do not copy our neighbors, but try to be an example. Our administration favours the many instead of the few: this is why it is called a democracy.” Popper describes Pericles’ words as follows:

. . . [N]ot merely a eulogy on Athens; they express the true spirit of the Great Generation. They formulate the political programme of a great equalitarian individualist, of a democrat who well understands that democracy cannot be exhausted by the meaningless principle that ‘the people should rule,’ but that it must be based on faith in reason, and on humanitarianism.

If Popper was a twentieth century intellectual herald for the open society, his was not an idea without other champions among the great philosophers of history. Immanuel Kant’s essay in 1795, “Towards Perpetual Peace,” embodies the idea of the open society based on autonomous individuals each acting according to his duty, according to the Holznens’ interpretation. This democratic ideal of an open society began to spread into practice following the horrors and devastation of world war brought on by tyranny and oppression.

“In the period following World War II, and accelerating after the end of the cold war, democracy grew and transparency norms spread across many nations,” the Holznens assert, a statement backed by Freedom House data showing 121 electoral democracies out of the world’s 192 states by the end of 2001, an increase of 44 in the span of 14 years.
The Promise of Transparency

The Holzners say that transparency is valued by those who seek freedom, “but it is not the open society; it is a value in information culture” [emphasis added]. The open society is vastly more complex. It stands for human rights and balanced values that include autonomy, accountability, privacy, and yes, responsible secrecy."23

Like other researchers who have studied the influence of transparency, the Holzners find the movement to transparency, certainly in the latter half of the twentieth century, is inextricably linked to the spread of democratic forms of government – a continuum that includes the founding of the United Nations and its Universal Declaration of Human Rights in 1948 and continues to the present day.

Lord, an international political science professor, lists the advancing of democratic governments among five factors that have been instrumental in the rise of global transparency. The others she names are: widespread availability of information technologies; the ascendancy of a global (and now digitally accessible) media; and the spread of both non-governmental organizations (NGOs) and international regimes (such as the World Trade Organization, World Health Organization, among many) that require governments of all sorts to disclose information.24

Like the Holzners, Lord, and others make a strong case for the connections between the values that support individual freedom and democracy and those that support transparency. The Holzners organized their views about the interrelationships among values, norms, technical and organizational infrastructures, and support systems into a “conceptual architecture of information value syndromes,” that include the following...
categories: values and countervalues; information norms; information infrastructures; and
general moral frames — contexts of the information value syndromes.\textsuperscript{25}

For the Holzners, the social values of transparency, privacy, autonomy,
accountability, secrecy, and loyalty are culturally dependent, and they concede that
societies differ in how they rank these values. In many cultures, however, transparency
— a “rising value” in their view — is “often in conflict with secrecy and privacy.”\textsuperscript{26} In
their analysis, “transparency is not a stand-alone social good, but part of a ‘syndrome of
values’ ‘dominated by openness of information and individual autonomy.’”\textsuperscript{27} With
individual autonomy comes the moral assertion to a right of privacy.

Lord describes the benefits of transparency as a facilitator of how shared values
are actually experienced, observing that “greater transparency also increases knowledge
of other peoples, which can increase tolerance toward others and decrease the likelihood
of conflict. When armed conflicts do break out, greater transparency may facilitate
grassroots support for intervention.”\textsuperscript{28}

Indeed, some researchers see transparency as supportive of freedom, and such
rights as privacy, as a result of its alignment with personal autonomy. Brin, for example,
comes at support of transparency from the skeptic’s perspective that maintaining freedom
– the ultimate democratic value in his view – in the Internet-driven information age is
what he calls ‘reciprocal transparency.’\textsuperscript{29} Rather than focusing on policies that would
shut down the flow of information in cyberspace, Brin argues it is preferable to
“compensate by opening them wider.”\textsuperscript{30} To illustrate his point, Brin suggests that
companies wanting to collect data on consumers online should have to post exactly the
same information about the top officers of the company and all their family members on an accessible website.

All of these researchers published their ideas before 2010, when the ‘Arab Spring’ revolutionary protests in Libya, Tunisia, and Egypt began, and Wikileaks released American diplomatic cables on the Internet. Yet, all of these writers agree that transparency supports individual freedoms, based on the ability of individuals to be self-directed and self-governing moral entities.

News coverage of the Arab Spring uprisings was filled with praise for social media’s role, notably Facebook, for keeping people connected, sharing information, and in general supporting bottom-up demands for change in a way that was never before possible. A study conducted at the University of Washington examining massive amounts of data found that social media “became a critical part of the toolkit for greater freedom,” according to Philip Howard, an associate professor of communications and the lead of the project team. The analysis was conducted by the Project on Information Technology and Political Islam, which is supported by the National Science Foundation and the George W. Bush Institute.31

Such global events as the Arab Spring protests speak to core benefits of transparency, just as Florini predicted in 2003:

Coupled with information technology, it [transparency] creates an explosive combination, one that could change the nature of governance as drastically as the print revolution did half a millennium ago. Where information technology, globalization, and democratization converge, we may be seeing the emergence of a dynamic new alternative to the coercive power of states: regulation by revelation.32
These societal-level values also play out on the person-to-person level. As Brin suggests, the transformation to a more transparent society “is not about eliminating privacy. It is about giving us the power to hold accountable those who would violate it.”

Brin was writing before the rise of social media, and he would probably be amused that for all Zuckerberg’s public blandishments about the virtue of radical transparency, its founder’s Facebook profile is not accessible to other users. (Perhaps Zuckerberg would counter that his ability to control who sees his personal page is also part of the design of Facebook.)

Facebook’s code and business model are largely driven by Zuckerberg’s personal philosophy, which includes the idea that the new era of digital information will promote human flourishing via radical transparency, perhaps the global governance model taken to the personal sphere. As a result, the site makes it difficult for users to make any distinction between personal and professional (or public) identities, let alone use a pseudonym. “You have one identity,” Zuckerberg says. “Having two identities for yourself is an example of a lack of integrity.”

If the promise of transparency is to aid in the global spread of individual freedoms, democratic governance, and greater accountability by the governed over those who govern, what are the threats to individuals and societies if this trend to transparency continues unchecked? And as the popular enabler of the transparent living experience for individuals around the world on the Internet, what lessons does the radically transparent Facebook experience offer?
Perils of Radical Transparency

While Lord’s analysis clearly describes transparency’s role in enabling greater social good in reducing uncertainty and increasing security by promoting broader understanding among groups in conflict, “greater transparency is not an unmitigated good,” she asserts.35

Transparency in her view has “two faces,” one of beneficence based on its capability to decentralize information — and the opposite, which is an essential instrument of control and power over people, via the selective use of shared information to support terrorist networks or an “illiberal regime,” or to “highlight widespread prejudice and hatred, encourage the victimization of out-groups” in ways that can actually lead the unwary to conclude there is “broad acceptance of such behavior without repercussions.”36 In short, transparency can be used to legitimize the illegitimate, and actually foster unethical treatment of groups and individuals.

As Lord points out, “the effects of transparency depend on what it reveals,” an obvious but nonetheless often ignored truth.37

Florini, Lord, and the Holznovers, among others, all agree that the Internet, and the rise of social media for individual communication and sharing in particular, has changed the equation in the balance between government control and citizen access. Some, like Lord and Brin, are also quick to point out that this new global means of information sharing has already shown its power to create outcomes that are negative as well as positive, for existing governments and their leaders, as well as for individuals.
A sampling of news and government accounts in the United States and around the world illustrates this yin-yang of transparency’s effects:

1.) Facebook profile pages were used to expand, and even direct, support for the American “Occupy” movement that began as a protest against Wall Street’s involvement in the nation’s financial woes beginning in 2011, and galvanized public opinion about the growing economic divide between haves and have-nots in America.

2.) Social media (including Facebook) fueled the protests in 2011 that later became known as the Arab Spring. The uprisings began in Tunisia, ignited literally by the self-immolation of a street vendor whose dignity had been grievously offended by a repressive government. Mohamed Bouazizi’s desperate act that led to his death in hospital a few days later set off street protests, which were captured on cellphone cameras and shared via social media, and spread rapidly across the Arab world thanks to Facebook’s widespread popularity.38

3.) A month after the Tunisian man set fire to himself and helped force a despotic ruler from power, the fatal beating of Khaled Said in Egypt that had taken place several months before helped to spark the mass protests in that country demanding the removal of Egyptian President Hosni Mubarak.39

4.) These same social media also are widely used by individuals and groups that sympathize with terrorist organizations trying to recruit new believers to their cause. In February 2012, the Senate Committee on Homeland Security and Governmental Affairs published a report that concludes as follows:

[W]ith the popularization of social networking sites, individuals who are becoming radicalized have the ability to find like-minded individuals more easily.
In addition, these social networking sites allow for a level of interaction and information sharing that was not feasible even a few years ago. Incendiary materials — including videos and lectures — are increasingly found not only on obscure websites but also on some of the most widely accessed sites in the world — including Twitter, Facebook, and YouTube. The result has been a pronounced increase in the volume of extremist material online, and a corresponding increase in the number of individuals who are viewing this material. 40

5.) Countless individuals using social media like Facebook for personal communications find themselves coping with unintended consequences in their careers and lives. Again, news headlines tell some of these stories: Of politicians who have been forced to resign after details of sexually explicit sharing of information or photos using Facebook or other social media became widely known. But public officials and well-known people from other walks of life are hardly the only ones who are ‘called out’ on their postings and pronouncements on Facebook.

6.) In fact, so pervasive have become the peccadilloes from use of social media that some media wags have taken to summarizing worst social media moves or “12 outrageous jobs losses due to mishandling social media,” as Ragan Communications headlined it in a 2011 online summary that included in the third-worst ranking the young woman who proudly Tweeted that she had been offered a good job at a well-known technology company in California: “Now I have to weigh the utility of a fatty paycheck against the daily commute to San Jose and hating work.” Needless to say, she didn’t get the job.41

Ragan, a leading trade publisher in the social media and communications industries, notes in a website article that the vast majority (89 percent) of U.S. companies indicate reviewing prospective employees’ use of social media as part of the recruiting
and hiring process. As mentioned in Chapter One, social media blunders frequently create inadvertent problems for people with public sector jobs, or those whose Facebook postings would cause most reasonable people to consider them inappropriate.

A case in point is the schoolteacher who lost her job over a photo on her Facebook page that showed her innocently toasting with a glass of wine at a restaurant. But other Americans have lost their jobs for not-so-innocently criticizing their bosses in posts to friends on Facebook that were (perhaps inadvertently) publicly available for viewing.

Since 2004, when Facebook morphed from Zuckerberg’s original creation of a way for Ivy League students to socialize (translation: meet girls), the portal has become a must-have tool for millions of Americans to communicate with friends and family. Over the years, Facebook’s privacy policies have morphed as well, from non-existent to various iterations that have earned it a reputation for publicly saying it is concerned about individual privacy, while at the same time adding services and features designed for maximum exposure (aka, radical transparency). Facebook provides privacy settings that are viewed as so complex that many users apparently give up trying to understand them, let alone deploy them to protect their personal information.

As it has mushroomed into a behemoth that in mid-2012 boasts 900 million user accounts worldwide, Facebook’s trove of data has exploded to rival that of Google. During these growth years, Facebook’s approach to the four categories of information handling that are involved in privacy considerations — collection, processing,
dissemination, and invasion — has confused and frustrated many users, privacy advocates and policymakers in the U.S. and Europe.

As recently as two years ago, only about 25 percent of users actively deployed Facebook’s privacy settings, according to its chief privacy officer, Chris Kelly. As Kirkpatrick observed in his book on the portal’s founding and early years, “many consider them [privacy settings] maddeningly difficult to use.”

In 2011, the tech-world media bible, *PC World*, published online a listing of “famous Facebook flip-flops,” including these attempts to take control of more of its users’ information:

**Flip 1**: On January 14, 2011, Facebook announced it would be giving developer partners the right to capture users’ home addresses and mobile phone numbers, if users checked ‘yes’ at the bottom of a permissions box, the same permissions box that appears when users logged in to a third-party website for the first time. This meant that the site’s numerous developer partners could access this personal data as well.

**Flop 1**: Following a weekend of online protests, Facebook reversed the decision. In a site blog post on January 17, Facebook acknowledged “we could make people more clearly aware of when they are granting access” to this sensitive information.

**Flip 2**: In August 2010, Germany’s Hamburg Data Collection Authority challenged Facebook’s use of email addresses of non-users who were invited to join the site as part of a feature called ‘Friend Finder.’ The German agency demanded to know how these emails had been obtained and how this information now in Facebook databases would be used.
Flop 2: In January 2011, Facebook agreed only to give German users a chance to opt out of future invitations and said it would issue them an explanation as to why they were being contacted. The site did not agree to stop capturing or retaining the email addresses.

Flip 3: One of the worst backlashes took place in April 2010, when Facebook decided to expand the user data it considered public (i.e., sharable with developer partners or advertisers), adding personal information that included city of residence, education, work, likes, interests, and friends.

Flop 3: After howls of protests and legal filings, Facebook announced it would overhaul its privacy settings. At a press briefing the following month, Zuckerberg said Facebook had simplified its privacy settings (from 50 down to about 15, with the number of sections from 10 settings on three pages to seven settings on one page). In the end, however, the broader use of data remained intact.

In all, PC World memorialized eight flip-flops that were among the privacy invasions which became part of the settlement the U.S. Federal Trade Commission announced it had reached with Facebook in late 2011. According to Kirkpatrick, this is really a reflection of the Janus-like posture of Zuckerberg himself, who the author says “considers himself a strong partisan for privacy rights,” at the same time “he also strongly believes that people are rapidly losing their interest in sequestering their data. So to keep the service in line with what he sees as changing mores, he continues to push Facebook’s design toward more exposure of information,” Kirkpatrick says.
In addition:

This contradiction helps explain the series of privacy-related controversies that have dogged the company throughout its history – around the News Feed in 2006, Beacon in 2007, the terms of service in early 2009, and the ‘everyone’ privacy setting in late 2009. In each case the company pushed its users a bit too hard to expose their data and subsequently had to retreat.50

Are these ‘changing mores’ to accept increasingly radical transparency in our online personal lives fully entrenched in American society, or European culture, or other societies around the world? If so, who now owns all the information about ourselves that we have shared online and is now archived by commercial interests there? And the central values question: What is lost if personal privacy is no longer available?

Some Internet experts say Facebook needs to determine how to protect its users’ privacy, especially in countries with restrictive regimes. The company's terms of use — which require members to use their real identities — make protesters vulnerable to government spying. Facebook chief executive Zuckerberg has insisted on the policy, saying the site would lose integrity if people hid behind phony identities.

"People at Facebook have been asking themselves in the wake of Egypt or Tunisia whether there might be a way they can allow political activities in these spontaneous revolts to acquire a little bit of anonymity," says Kirkpatrick. "The problem is, if they start making it easier for political activists to use Facebook in places like Egypt or Tunisia, those same capabilities are likely to be used by people we don't admire or pro-government thugs."51

As we have seen, the value of transparency or privacy lies in what is being shared; in other words, context is everything. Because of its vast size, Facebook now sets the path
for others to follow, whether the issue is privacy settings and controls, or what data Facebook makes available to other commercial partners and advertisers. A recent post on the social media marketing site, Mashable.com, notes that Facebook users post nearly 685,000 pieces of content (photos and posts) per minute.52 No wonder the company’s servers, located in various places around the world, now number in the mid-five figures.

At the societal level, Facebook represents a monumental mixed blessing. Yes, it brings together people who are seeking to promote human rights or freedom from repression; but it also is used by terrorists and others who espouse violence and harm to influence and recruit followers. Governments around the world routinely censor and cut off access to the Internet and social media, including Facebook, as part of efforts to ‘control’ the populace at times of unrest.

At the individual level, Facebook presents the same dual capability to support social goods as well as facilitate social harm. Yes, it makes it easier for people to stay in touch, to renew contacts with long-lost friends and family, and engage in rallying support for good causes. It also reaps embarrassment and humiliation when too-personal images and postings are shared too widely, and even makes it easier for bad behavior like bullying and hate-speech to proliferate online and cause harm to countless innocent individuals.

As Kirkpatrick, Facebook’s biographer, notes: “The amount of data about us that resides on Facebook . . . raises public policy questions about privacy. Should this company — or any one company — control and aggregate so much inside its own infrastructure? Should that be a job for government?”53
The case for a balancing between the social goods of transparency and privacy is clear. Neither a democracy nor its citizens’ autonomy can achieve their fullest expression without appropriate boundaries between this pair of important social values. Though democratic societies, and individual citizens, will draw boundaries differently among these social goods, the framework that makes possible these choices should remain strong.

Brin gets to the heart of where the balance should lie when he notes that “privacy is a highly desirable product of liberty. But accountability is no side benefit. It is the one fundamental ingredient upon which liberty thrives.” Although he was making this argument as a passionate call for greater transparency, he later thoughtfully adds the key point mentioned earlier that “[t]ransparency is not about eliminating privacy. It is about giving us the power to hold accountable those who would violate it.”

In democratic societies, the power to hold accountable is leavened with the right combination of legislative and regulatory safeguards, bolstered by a legal system of tort law that provides an additional restraint.

The next chapter will examine the lessons that can be extracted from European views of privacy and the European Union’s policy and legal framework to protect citizens’ rights to privacy online alongside freedom for Internet commerce and social sharing.

With the European model as a backdrop, several approaches will be reviewed that can contribute to a new policy model for privacy in the United States, including perspectives on the current Obama administration’s Privacy Bill of Rights, and how a
stronger statement of privacy principles might serve to support legislation that strengthens contextual privacy and reciprocal transparency.
Chapter Four
Privacy: Balancing Freedom and Autonomy

The deep meaning of personhood is being reduced by illusions of bits. Since people will be inexorably connecting to one another through computers from here on out, we must find an alternative. Next to the many problems the world faces today, debates about online culture may not seem that pressing. But digital culture and related topics like the future of privacy . . . concern the society we’ll have if we can survive these challenges.1

— Jaron Lanier, You Are Not a Gadget: A Manifesto

When he published these words in 2010, Lanier was sending a cri de coeur to everyone who goes online to do so mindfully and thoughtfully in the Web 2.0 era of user-generated online content. Later that year, well-known legal commentator on the future of technology, Jeffrey Rosen, wrote in a New York Times essay that even hiring a reputation management expert to “tweak your Google profile” may be insufficient as Web 3.0 turns into “a world in which user-generated content is combined with a new layer of data aggregation and analysis and live video.”2

Rosen points out that Facebook is actively engaged in aggregating its vast trove of photographs, acquiring companies and building developer partnerships aimed at using new technologies for facial recognition combined with social-connections software. Rosen sees Facebook’s activity as leading the way to a dystopia in which Internet searches for images of specific individuals will damage countless lives, whether intentional or unintentional:

[These searches] are likely to be combined with social-network aggregator search engines . . . which combine data from online sources – including political contributions, blog posts, YouTube videos, Web comments, real estate listings and photo albums. Increasingly these aggregator sites will rank people’s public and private reputations.3

70
Rosen notes that legal experts are already anticipating these challenges as they look at how U.S. statutory and regulatory policies can be fashioned to help preserve privacy for individuals, families and children, and correct the damage that is already affecting personal reputations and lives from ungoverned uses of people’s personal information.

Clearly, the Internet is hosting a fast-changing virtual world of opportunity for those who would seek to profit from the vast amounts of data, including images and information of all kinds, even the social postings and photos millions of Americans put there every hour of every day. Absent concerted action by policymakers to change the current dynamic, Facebook’s radical transparency appears to be enabling a personal data bonanza for the online marketplace, made possible by the Internet’s current architecture and gaps in the law. Social norms, as often as not, follow the changes in the other three constraints on behavior in cyberspace that Lessig first described. No wonder so many privacy researchers open their discussions by lamenting the murkiness and complexity of today’s fast-moving privacy concerns.

However, a comparative cultural view of privacy policy in the digital information age can reveal fresh perspectives, as happens when the American and European approaches to privacy are looked at relative to one another. This chapter will review European societies’ conceptions of privacy, as well as the contemporary framework for the European Union’s current digital privacy rights.

Next, all of the insights about privacy in America – from its historical and legal roots to moral and philosophical value to a look at radical transparency’s decidedly
mixed potential as a social norm – will inform a discussion of what is needed to bring
greater balance to the competition among rights of freedom and privacy. The final section
will look at the current state of efforts by American policymakers and government
leaders to seek improvements to business practices, laws and regulations to strengthen
protection for citizens’ personal privacy in the information age. Interestingly, the
principles that emerge in the U.S. have much in common with current EU policies, and
would set America on a path toward greater equilibrium among cherished rights,
including the implicit right to privacy.

European Views of Privacy

Viktor Mayer-Schönberger takes a detailed look at trends at work in both Europe
and the United States, and declares that “Americans have no federally codified general
right to information privacy vis-à-vis any body outside the federal government,”\(^4\) a bit of
an overstatement, as current U.S. privacy law certainly protects the privacy of education,
medical and financial records as well. In contrast, he maintains European legislatures
“were bolder (perhaps due to the long shadow cast by Europe’s violent and brutal
twentieth century history), and so empowered individuals with information privacy rights
not just vis-à-vis central government, but all public and private sector information
processors.”\(^5\)

Mayer-Schönberger was repeating what a number of legal scholars and privacy
researchers have taken as a ‘given’ about the differences between American and
European views on privacy; namely, that the terrible human devastation caused by
fascism and totalitarianism in Europe in the 1930s and 1940s is the foundation of today’s comprehensive EU legal protections of individual privacy.

Frequently cited in these discussions is the case of the Dutch government, which created a population registry in the 1930s that contained name, birth date, address, religion, and other personal information on every citizen. At the time, it was praised for its ability to facilitate government welfare planning and administration for citizens. But tragically, when the Nazis overran the Netherlands and took control of the government, this registry was used to identify and persecute Jews and gypsies, among others. Mayer-Schönberger notes that the result was the Nazis were able to deport and murder a significantly higher percentage of the Dutch Jewish population (73 percent), than any other European nation, including Belgium (40 percent) and France (25 percent).⁶

He uses this horrific example in his argument for strong privacy protections, including automatic end-dates for personal information storage and the right to delete one’s digital information. “We do not know what the future holds in store for us, and whether future governments will honor the trust we put in them to protect information privacy rights,” Mayer-Schönberger says.⁷

However, some historians look farther back in history to see the foundations of European and American differences in how liberty values are expressed today. Even though Holland’s terrible twentieth century experience is a pointed illustration of the fear that stokes Americans’ historical distrust of government, Garry Wills contends in his thorough analysis that Americans live with a largely “mythical history” that the
Constitution was deliberately cast to be inefficient in order to support a shared distrust of central government power.8

Wills argues persuasively that Americans are imbued with their love of liberty, mainly in the forms of freedom of the press and freedom of speech, and their distrust and disregard for government, based on a largely mythologized view of the nation’s history from Revolutionary times through the creation of the Constitution. From the eighteenth century onward, Americans saw free speech and a free press as the ultimate bulwarks against government tyranny that could appear at any moment.

“Self-government by the individual was so intensely desired that government by others — even by legitimately chosen representative others — was, in many incremental ways, delegitimized,” Wills writes, summarizing why Americans to this day tend to value individual liberty over government involvement in protecting other important rights, in this case the right to control access to and use of one’s personal information.9 There is strong consensus among privacy researchers that Americans consider this interpretation of liberty to be their preeminent social value, and therefore, the U.S. legal tradition tilts toward freedom of speech and the press over privacy rights.

In contrast, the European tradition is grounded in respect for dignity, which some researchers refer to as ‘reputation,’ and consequently leans heavily toward government regulation to preserve citizens’ control over their personal information, or any depiction of them in public. Eminent comparative legal scholar James Q. Whitman argues persuasively that Europe and America have differing privacy cultures based on their social and political histories. Whitman observes that “the sense of what must be kept
‘private,’ of what must be hidden before the eyes of others, seems to differ strangely from society to society,” and would seem inexplicable until one examines the full scope of a society’s cultural history.10

“If privacy is a universal human need that gives rise to a fundamental human right, why does it take such disconcertingly diverse forms?” he asks.11 Whitman then offers an insightful response:

These are not questions we can answer by assuming that all human beings share the same raw intuitions about privacy. We do not have the same intuitions, as anybody who has lived in more than one country ought to know. What we typically have is something else: We have intuitions that are shaped by the prevailing legal and social values of the societies in which we live.12

In his view, differing approaches to privacy grow out of “much larger and much older differences over basic legal values, rooted in much larger and much older differences in social and political traditions.”13

Europeans, according to Whitman, derive their contemporary social values of dignity and autonomy from deeply rooted legal and social history going back to the monarchies and aristocracies of the seventeenth and eighteenth centuries in which norms of personal honor were legally enforced for citizens of high status. By the early twentieth century, what he terms a “leveling up” had begun across European jurisprudence that applied these norms to all citizens. “Continental privacy law is, as it were, ‘society’ privacy for everybody.”14

This helps to explain why Europeans place such emphasis on maintaining control over their public image, and have an honor-oriented suspicious attitude toward a free press and free market. Whitman describes the history of the continental law of respect as
“closely linked with the history of continental etiquette, which also began as a set of rules for courtiers, only to be generalized to the entire population.”

At the heart of the different social values of Europeans and Americans is how the two cultures intuitively understand the imperatives of ‘personhood,’ or of ‘the integrity of the person.’ ‘One’s sense of personhood can be grounded just as much in an attachment to liberty as in an attachment to dignity,’” Whitman notes.

To illustrate these differences: Europeans view personhood as confirmed when bosses must respect their privacy in the workplace, and they have the right to sunbathe naked in a public park; and Americans feel their personhood is respected when they are free to protest against unfair taxation, and keep loaded weapons in their homes.

Whitman believes these differences should not lead to a conclusion that one is right and the other wrong, “that one side of the Atlantic has discovered true ‘personhood,’ while the other lags behind.” In fact, he sees no logical inconsistency in pursuing both forms of privacy protection. “It is perfectly possible to advocate both privacy against the state and privacy against nonstate information gatherers — to argue that protecting privacy means both safeguarding the presentation of self and inhibiting the investigative and regulatory excesses of the state.”

The United States has the First Amendment to the Constitution to protect freedom of expression from government intrusion, just as Europe has the Human Rights Convention to guarantee this freedom. But as we have seen, America has no equivalent to the Charter of Fundamental Rights of the European Union, adopted in December 2000, in which “the right to respect for his or her private and family life, home and
communications,” is expressly granted.\textsuperscript{19} In the U.S., the right to privacy is implied in several of the first Constitutional amendments, but has remained subservient to liberty rights, much to the dismay of contemporary privacy advocates.

So embedded is the idea of individual privacy as a fundamental human right to Europeans that even as the new EU Charter was slowly winning member states’ approval, the EU Privacy Directive was approved in 1995, which spells out in detail the rights of EU citizens to exercise control over their personal information. These rights include requiring that personal data can be processed only when the individual has given explicit consent; the right to correct any information collected; and the requirement that the data be kept in a form that permits removal of personally identifiable information after the purpose for which the data was collected has been served.\textsuperscript{20}

The practical implications of the EU Privacy Directive loom large for the mostly U.S.-based Internet giants of social media and search, including Facebook and Google, as interpretations and additions to the Directive have continued as these companies have advanced their own efforts to market new services and uses of their enormous information databases.

Since Viktor-Schönberger wrote in 2009 of the terrible risks to societies on both sides of the Atlantic if sites on the Web are permitted to permanently archive personal information, the EU has moved to provide further ‘delete’ options and protections for its citizens. Under the leadership of Viviane Reding, EU justice commissioner, Europe is advancing further changes to e-privacy rules containing stronger safeguards for individuals’ control over their information, including ‘right to be forgotten’ requirements,
and harmonizing individual member state data protection directives and activities under a single EU-wide authority with an implementation target of mid-2013. As the European Consumer Organisation (BEUC) notes in its comments to the latest draft of the new privacy rules, BEUC welcomes “enhancing the rights of data subjects and restoring control over the processing of their own personal data, especially in light of constantly evolving information computer technology developments.”

In general, the EU privacy changes are aimed at: strengthening meaningful consent requirements; enforcing transparency principles on any entity (whether located in the EU or not) that would collect or process individuals’ information to communicate their practices and requests in clear and simple language; encouraging privacy ‘by design’ in the development of online services; and strengthening purpose limitation to control the currently unregulated transfer of individuals’ information and profiles among Internet providers, including social networking sites and search engines.

In 2011, for example, 90 Spanish citizens petitioned its Data Protection Agency to have their personal information deleted from the Web, including a victim of domestic violence who discovered her address could easily be obtained online, and another who thought it unfair that an arrest from her college days was also available online. “I cannot accept that individuals have no say over their data once it has been launched into cyberspace,” said Reding, the EU’s justice commissioner, in promising to see the new ‘right to be forgotten’ rules put into effect.

The advantage of the new Directive to companies doing business with, or providing services over the Internet to, EU citizens is that they will be dealing with a
single EU-wide data protection authority under a unified set of regulations. However, this efficiency advantage has not deterred U.S.-based companies from pressing Brussels to ease up on new restrictions on their processing and use of data on individuals, on the grounds that it will be far too technically complex to develop the infrastructure needed only to comply with European directives. "This (referring to the EU proposal) is the battleground right now," said John M. Simpson, the Privacy Project director at Consumer Watchdog. "In this global, digital, highly interconnected world, it quickly becomes the case that companies want harmony in their standards. So, if the Europeans continue to press their stand for basic human privacy rights, that will set a standard that will go worldwide and have tremendous benefits for the U.S. consumer."  

Even as the lobbying and discussions continue over the EU e-privacy proposal, Germany is reopening its investigation into Facebook’s privacy practices, and pressure from the Irish data protection office resulted in a recent Facebook decision to suspend the facial-recognition tool that suggests when registered users could be tagged in photographs put on the site.

Clearly, Europeans’ sensibilities about the value of privacy continue to drive robust EU policy engagement to keep up with the fast-paced developments of the Web 2.0 world. Some U.S. privacy advocates are on record saying they are pinning their hopes for stronger privacy protections in the United States on the popular support that the European privacy proposal has among Europeans. If the EU enacts the bulk of its current plan, U.S. advocates are betting it will benefit privacy controls in the United States, if for no other reason than Internet-based commerce and communication is global, and
separating social users or customers by their country identifiers for separate privacy permissions and treatment would be too costly and complex an undertaking for the U.S.-based Internet companies to achieve, therefore they would settle for code-writing for the more restrictive requirements.

However, Nicole Lamb-Hale, assistant secretary of the International Trade Administration of the U.S. Commerce Department, testified before a House Energy and Commerce subcommittee, that the United States is unlikely to adopt the EU approach, and instead will continue under the EU-U.S. negotiated safe harbor framework that took effect in 2000, which allows U.S. businesses to self certify and declare compliance with an agreed-upon set of privacy principles. Interestingly, Lamb-Hale added that U.S. online businesses should be willing, for competitive reasons, to accept privacy principles that are sufficiently flexible.26

Transatlantic differences over privacy values continue, in other words. “The two cultures really aren’t going in the same direction when it comes to privacy rights,” a Georgetown University law professor, Franz Werro, told The New York Times. Werro, who was born and reared in Switzerland, explained that Europe sees the need to balance freedom of speech and the right to know against a person’s right to privacy and dignity, while in America, courts have consistently found that the right to publish the truth about someone’s past supersedes any right to privacy.27

Today, every European country has privacy laws protecting individuals in the marketplace, along with Australia, Canada, and many Latin American countries. Only the
United States limits individual privacy protections to government records, health and financial records, and oddly, movie rental records.

**Lessons and Options**

In examining the ethical implications of Facebook’s radical transparency on the future of privacy in America, several important principles emerge that need to be emphasized in the light of the central values question: *What is lost if privacy is no longer available?*

Clearly, transparency is a social good. In particular, openness benefits citizens in their dealings with government because it acts as a constraint on government exercise of authority over the people. Transparency in interpersonal relationships also serves as a valuable light to inform understanding, and avoid conflicts based on lack of appreciation for the views and beliefs of others.

However, in an extreme form, as Facebook exemplifies in its continual launch of features designed to promote total exposure of information, radical transparency poses two persistent and serious threats to individuals and society at large: first, the ever-present threat of exposure of personal information in inappropriate contexts; and second, the use of the personal data of millions of people by a rapidly growing number of third parties for purposes well beyond the original intent or control of those individuals. The consequences of the data aggregation industry’s activities are largely unknown, and therefore, should be regarded with more than a little skepticism by government and citizens alike. Despite Facebook’s repeated retreats in the face of government calls (both
in the United States and Europe) of privacy violations, the social media site continues to press its philosophy of radical transparency onto its millions of users.

Facebook’s radical transparency fails as an appropriate model for a social good in the information age because it unilaterally erases the line between public and private communication, denying the opportunity for individuals to decide where the boundaries should be drawn, and what standards should guide the new normative foundation for public and private communications in the Internet era.

The site’s refusal to accommodate the needs of activists organizing protests against tyrannical regimes to protect their true identities on the social media site is but one example of how Zuckerberg’s insistence on ‘one identity’ collides with the grim reality in many parts of the world. In addition, Facebook’s insistence on ‘forever’ accumulations of data and images threatens an Orwellian outcome in which, as Mayer-Schönberger describes, citizens may find themselves in a world in which their autonomy and that of their children is constrained by the eternal nature of digital remembering:

Will our children be outspoken in online equivalents of school newspapers if they fear their blunt words might hurt their future career? Will we protest against corporate greed or environmental destruction if we worry that these corporations may in some distant future refuse doing business with us? In democracies, individuals are both citizens and consumers.28

It is vitally important that carefully thought-out restraints on unilateral decision-making by business interests, especially when they force such extremes of transparency on society, be put into place that will enable the restoration of the balance between the rights of individuals to control information about themselves and the other important freedoms they enjoy in a democratic society. This is even more imperative as the Web
2.0 era of user-generated content evolves into whatever Web 3.0 will bring in the era of ‘big data’ collecting, tracking, monitoring, and aggregating.

The examination in this paper of the current state of privacy rights in America has shown that the four ethical constraints on cyberspace are not currently acting in the best interests of individuals’ rights to an appropriate level of control over access to their personal information. U.S. law presently provides inadequate Internet privacy protections for adults and children. Code-writers and market forces aggressively seek new and more effective ways to commercialize the data troves that comprise the details of the lives, habits, interests, fears, and desires of billions of people around the world.

The fourth constraint, social norms, varies by culture and recent history suggests these norms are sometimes influenced by the relentless pressures of the marketplace. Surveys show most Americans consider privacy an important value, but this view could be trending toward a general practice of acceptance of less privacy in the giddy early years of social networking combined with online shopping. Even though U.S. consumers endorse the idea of privacy controls, paradoxically many are willing to trade away this control for even a modest perceived benefit offered by an online merchant, regardless of whether the lure is presented by a well-known, established brand or less-trustworthy one.

As Nissenbaum describes, social media sites like Facebook pose two serious privacy issues by erasing the boundary between public-private communication: first, the problems that arise from self-exposure of personal information and the exposure of personal information about others; and second, the current state of unilateral privacy policy-setting by Internet companies, led by Facebook as the leader in social media.29
If these trends continue, there will be ever-diminishing privacy online, and what will be lost will be measured in the years to come as an erosion to the value of personhood and autonomy for individuals in American society as well as to important “pluralist values” of the larger culture, as Solove points out, which include the promotion of civility, the modulation of disruptive invasions, and protection of all manner of activities, “from the worthy to the wicked,” without which “the friction of society might increase, potentially igniting into strife and violence.”

Viewed on the personal level, most scholars conclude that individual privacy is an essential benefit of liberty. It supports the fullest development of human potential, creativity, and individualism, and is a form of protection against society’s worst tendencies to oppression by majoritarian social convention. Privacy not only protects the individual against prejudicial norms of society, but also supports society’s beneficent norms by promoting and protecting the social civilities that define and strengthen community.

Solove’s recommendation that U.S. law consider a pluralistic approach that includes European-style reputational impacts based on the blurring of public-private communication boundaries online; and Nissenbaum’s proposal that online information should be protected according to the norms that govern distinct social contexts are two valuable theoretical and decision-framing constructs for policymaking.

Neither of these ways of looking at privacy policymaking precludes use of the other; in fact, each can be applied to ensure equilibrium is maintained as digital technology continues to advance and the Internet evolves.
In America, privacy tilts toward protecting individuals against the worst intrusions by government; and in Europe, it emphasizes protection of the individual’s dignity and reputation. If nothing about us is off limits and unavailable to others on the Internet, as radical transparency supposes is a social good, then these precious preserves for individualism and dignity are eroded, if not lost, over time.

The American and European forms of privacy are not mutually exclusive, as Whitman rightly observes, and can be reasonably applied through the four forms of constraint on cyberspace to achieve a more appropriate balance among equally important, but sometimes competing, freedoms. In fact, at least one set of principles have been put forward in the United States, by a White House task force, that closely align with those of Europe, even though acknowledging this publicly would not be politically advisable based on the longstanding cultural divide described earlier.

As the review of the privacy literature illustrates, there are several promising approaches and infrastructure tools for U.S. policymakers to consider as they go about deciding how best to adjust the levers to achieve balance among restrictions, incentives, and protections for Internet operators and businesses; developers of Internet infrastructure, software, and hardware; and individuals, including parents and their children.

Among the most promising are those that rely on a combination of technical architecture changes, or code, aligned with appropriate policy requirements and market incentives. In the United States in particular, citizen-consumers have been on their own to police their data profiles on the Internet without sufficient tools to help them manage
their online interactions. Far too often the only remedy available to the average person is a costly and time-consuming tort action (or threat to file a lawsuit) to assert rights over personal information or resolve a harm resulting from a privacy invasion.

Such a ‘you’re on your own’ approach would also occur if the policy answer is a contractual rights remedy, for example, which some experts have recommended in recent years. ‘Propertized’ personal information sounds like the perfect solution in the U.S., where freedoms of the market and expression often trump privacy. A ‘personal trademark’ approach also could be accommodated technically, within current digital rights management (DRM) architectures, like the systems used to secure online copyright protections for music. But it would be overwhelming to manage for the average person.

As Mayer-Schönberger points out, a DRM approach amounts to a “blunt tool” when something with much greater precision is required to protect a single individual’s personal information.31 Like several other privacy and security experts, he mentions the near-future possibility of new privacy management systems that would enable individuals to negotiate usage parameters of their information with specific providers. 32

Even today, privacy enhancing technologies (PET) are available for use on the Internet, as Lessig points out, including a protocol known as P3P, or Platform for Privacy Preferences, which resides on the individual’s computer and provides a machine-readable set of privacy preferences wherever that person goes online. This technology, discussed in Chapter Two, is being tested and evaluated further, but is already available as a solid user-friendly tool.
Software using PET, for example, could be combined with Mayer-Schönberger’s recommendation for purpose limitations on individual data collection and storage. Under this approach, user and provider would agree in advance on the uses for the information. Such a system also could include expiration dates, and even a delete-at-will clause for the owner of the information. The latest EU privacy proposal moves in this direction, including a plan to encourage PET, and also spells out the principle of ‘the right to be forgotten’ online.

A combination of competitive carrots and regulatory sticks could be deployed in the United States as well to bring more order and balance to the current online free-for-all environment. User-friendly PET tools like the P3P software could be encouraged by policies that provide market incentives to Internet platform providers and online businesses to develop and make them available to customers and users.

In addition, further collaboration between government and the private sector to take the next steps beyond the White House task force that produced the “Consumer Privacy Bill of Rights” earlier this year would be another welcome action toward bringing more balance between privacy rights and other freedoms. It would have the advantage of bringing representatives of powerful market players to the policy discussion table.

Ultimately, whether by policy design or a voluntary market ‘best practices’ approach, the U.S. should consider appropriate purpose limitations, expirations, and deletion rights on individuals’ information to deal with the most serious threats from use of social networking sites that have surfaced so far, including: social norm violations of
public-private boundaries; inappropriate controls on children’s use; and unfettered personal data collection and aggregation by site providers like Facebook and its third-party developers and aggregators.

These options can be modulated to maintain a high degree of transparency, or openness in online communications for business purposes and social networking, while at the same time providing a new framework in which individual citizen-consumers have the ability to make better choices for themselves and their children. Mayer-Schönberger explains the likely outcome if nothing changes this way:

As digital memories make possible a comprehensive reconstruction of our words and deeds, even if they are long past, they create not just a spatial but a temporal version of Bentham’s panopticon, constraining our willingness to say what we mean, and engage in our society. Do we really want to live in a society of servility and fearfulness?33

Current U.S. Policy Direction

Clearly, the European Union approach to privacy illustrates principles that can be applied to restore balance among sometimes competing rights in America, both for individuals and the larger social good. And although policymakers on both sides of the Atlantic share a number of common concerns, it remains to be seen whether Americans can overcome their long-held political distrust of any idea that can be branded as emanating from a European sensibility. There are some encouraging signs, however. First, there are the principles embodied in the White House task force’s “Consumer Privacy Bill of Rights,” which align with EU proposals, and recent activity suggests that the U.S. shares an urgent concern with Europeans about what the technology future will mean for the young.
The EU proposal contains new rules to aid parents of children under age 13 in protecting them against online predators and overexposure of personal information, and similar fears in the United States recently resulted in a bold response by the Federal Trade Commission (FTC):

In September, the FTC’s Mary K. Engle said the agency is proposing tougher rules to respond to the rapidly spreading practice of data aggregation by Internet companies and social networking sites out of concern that the data and activities of millions of young users are being collected and put to various uses without their parents’ awareness or consent.\(^\text{34}\)

Such data-mining practices are currently unregulated in the United States, and the FTC is moving quickly to remedy this, at least for children under age 13, Engle said. “Today, almost every child has a computer in his pocket and it’s that much harder for parents to monitor what their kids are doing online, who they are interacting with, and what information they are sharing,” she said.\(^\text{35}\)

The FTC is proposing the first changes in more than a decade to the Children’s Online Privacy Protection Act (COPPA) that would require Web operators of children’s sites to obtain parental consent before they collect personal information such as phone numbers and addresses, and to use ‘cookies’ to track children’s activities on the Internet. The move quickly drew strong opposition from Facebook and other Internet giants on First Amendment and technical complexity grounds. The industry’s response is that tougher children’s privacy laws “could hamper America’s ability to ‘like,’ tweet and

89
share information across the Web,” undermine free speech rights, and pose undue burdens on platform providers.\textsuperscript{36}

Facebook, in a written response, said the FTC proposal “raises First Amendment concerns,” and that the rule changes are unworkable given the ubiquitous nature of links among sites on the Web, including children’s sites. Facebook has a minimum age limit of 13, but two years ago, Consumer Reports determined that at least 7 million under-age children were Facebook users, a figure many experts today consider extremely conservative.\textsuperscript{37}

Advocates for children and privacy immediately fired back at the giant Internet companies, including Facebook, Google, Twitter, and Apple, arguing that they need to accelerate efforts to protect children’s privacy online. “It’s a pathetic argument for the richest companies in the world to say they don’t have the resources or ability to protect children,” said Jim Steyer, head of Common Sense Media, a child advocacy group in California and a professor at Stanford University.\textsuperscript{38}

Common Sense Media is collaborating with another advocacy group, the Center for Digital Democracy, to advocate on behalf of the FTC’s proposed changes to COPPA, and to provide a counterweight to the arguments of the major Internet companies.\textsuperscript{39}

This latest fight between powerful commercial interests and public and non-profit advocates for children illustrates the entrenched players that align against every effort to strengthen privacy protections for individuals. Commercial market forces have staked out large territories on the Web 2.0 Internet, and many business experts believe companies like Facebook are only just beginning to develop profit models based on their data troves.
With the exception of the FTC’s push to overhaul the U.S. children’s online privacy law, none of the other 19 or so legislative proposals in circulation during the latest session of Congress have moved forward, though some privacy advocates have suggested this may change after the November 2012 federal elections.

The legislative proposals mentioned in Chapter One that remain stalled as the 2012 congressional year winds down include bills aimed at providing citizen-consumers with more protection against online tracking; similar protections against geolocation surveillance; and tighter standards for collection and use of personal information. Many of these measures are consistent with the Consumer Privacy Bill of Rights introduced by the White House earlier in 2012 that also was mentioned in Chapter One.

This statement of rights has much in common with the EU proposal, including the important concepts of reasonable limits and contextual integrity on the collection and use of personal data. Whether Congress will pursue legislative proposals based on these principles remains to be seen. But at least one state is not waiting to see what the final ‘lame duck’ Congressional session of the year might bring.

California, which leads the nation in innovative legislation on a variety of social and environmental policy fronts, recently became the first state to enact laws protecting both students and workers from requirements by school administrators or employers for access to individuals’ social networking sites if their privacy settings keep what is there hidden from public view. Maryland and Illinois voted to ban employers from requesting access to employees’ (or prospective employees’) social media accounts, and Delaware has a similar law protecting students’ rights to social media privacy. About a dozen other
states are considering similar legislation, in addition to a proposal languishing in Congress. According to data compiled by the National Conference of State Legislatures, at least 10 states have privacy statutes that apply to private-sector entities’ online treatment of individuals, and 16 states have privacy laws to regulate government online interactions with citizens and their personal information.

This suggests that U.S. policymakers, whether beginning at the state level and migrating to the federal level, are focusing more attention on the need to shore up privacy protections for their citizens. FTC Commissioner Jon Leibowitz, in testifying before the Senate Committee on Commerce, Science and Transportation in May 2012, emphasized the importance of educating the public to be cautious as citizens and consumers online, and at the same time encouraging the Internet industry to adopt meaningful privacy best practices. “This is a critical juncture for consumer privacy, as the marketplace continues to rapidly evolve and new approaches to privacy protection are emerging in the United States and around the world,” Leibowitz told the Senate panel.

The U.S. agency, he said, encourages the private sector to pursue a “privacy by design” approach (identical to that of the EU) to build in best practices in their transactions with users and consumers, including providing simpler and more streamlined choices about the company’s data practices; and taking steps to make data practices and data uses more transparent to consumers, including simplifying and standardizing privacy policies so that these policies can be more readily understood and compared.
There is little doubt that such steps, if taken voluntarily by Internet businesses, would strengthen privacy for everyone who goes online to socialize or conduct business. The carrots and sticks may, in the end, make all the difference, as Rosen suggests. The law professor at George Washington University recently wrote that the EU’s proposed ‘right to be forgotten’ rules are being “strenuously resisted” by Facebook and Google in Brussels. His observation on this coming “titanic clash” is as follows:

The Europeans may be going overboard in creating a new legal right to escape your past on the Internet, but if the threat of regulation prompts Facebook and Google to explore less heavy-handed ways of empowering users to clean up their online reputations, perhaps Europe and America can find some kind of common ground after all.44

Rosen’s conclusion is certainly the best hope for U.S. privacy advocates. Until then, Americans still remain mostly on their own and well advised to take Lanier’s advice to share any information online mindfully and thoughtfully, and to teach their children well about the perils of online social networking, especially on Facebook. It is clear that radical transparency fails as a social norm worth passing on to the next generation.
ENDNOTES

Chapter 1


2. Ibid., 193.

3. Ibid., 195.


6. Ibid., 193.

7. Solove, Understanding, 176.


9. Ibid., 12.

10. Ibid., 13.

11. Ibid.

12. Ibid., 5.


18. Ibid., 26.

19. Ibid., 77.

20. Ibid., 78.

22. Ibid.

23. Ibid.


25. Ibid., 179-180.


28. Solove, Understanding, 179.


30. Ibid.


32. Ibid.


34. Ibid.

35. Solove, Understanding, 1.

36. Ibid.


48. Ibid.


Chapter 2


5. Ibid., B8.

6. Nissenbaum, Privacy, 63.


12. Ibid.


14. Nissenbaum, Privacy, 70.

15. Ibid., 71.

16. Ibid.

17. Ibid., 81.


19. Ibid.


21. Ibid.

22. Regan, Legislating, 221.

23. Ibid., 225.

24. Ibid., 221.

25. Ibid.

26. Ibid., 227.
27. Lessig, Code, 7.

28. Ibid.

29. Ibid., 124.

30. Ibid., 219.


35. Ibid.


40. Ibid.


42. Ibid.

44. Ibid.


46. Ibid.


49. Ibid.


52. Ibid., 54.

53. Ibid.

54. Ibid.

55. Ibid., 55.

**Chapter 3**


2. Ibid., 200.

3. Ibid., 324.

4. Ibid.

5. Ibid., 325.


8. Ibid.

10. Ibid., 17.


16. Ibid.


26. Ibid.

27. Ibid., 10.


30. Ibid., 81.

32. Florini, Coming Democracy, 34.


34. Kirkpatrick, Facebook Effect, 199-200.

35. Lord, Perils and Promise, 3.

36. Ibid.

37. Ibid., 117.


42. Ibid.


44. Ibid.

45. Kirkpatrick, Facebook Effect, 208.

46. Ibid.


48. Ibid.

50. Ibid.


55. Ibid., 334.

Chapter 4


3. Ibid.


5. Ibid., 137.

6. Ibid., 141.

7. Ibid.


9. Ibid., 17.


11. Ibid., 1154.

12. Ibid., 1160.

13. Ibid.

15. Ibid., 1167.

16. Ibid., 1163.

17. Ibid., 1164.

18. Ibid., 1219.


28. Mayer-Schönberger, Delete, 111.

29. Nissenbaum, Privacy, 221-222.


31. Mayer-Schönberger, Delete, 150.
32. Ibid., 151.
33. Ibid., 197.
35. Ibid.
37. Ibid.
38. Ibid.
43. Ibid.
BIBLIOGRAPHY


Madden, Mary. “Privacy Management on Social Media Sites.” Pew Research Center, Pew Internet & American Life Project.


