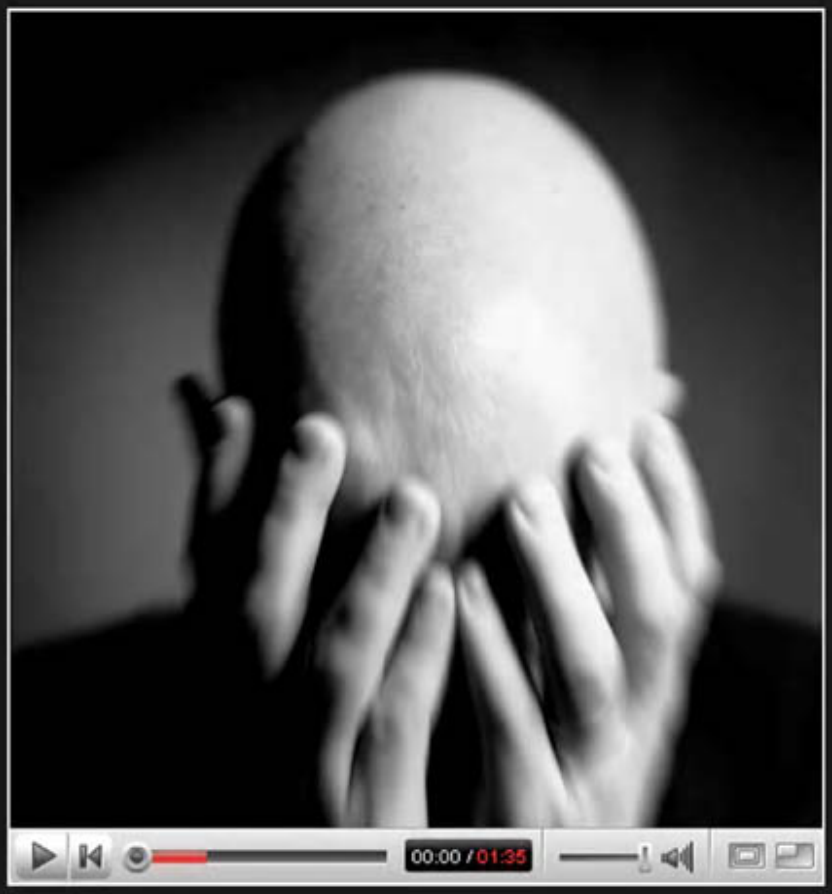
the future of reputation

gossip, rumor, and privacy on the internet



Daniel J. Solove

The Future of Reputation

This page intentionally left blank

The Future of Reputation

Gossip, Rumor, and Privacy on the Internet

Daniel J. Solove

Yale University Press
New Haven and London

To Papa Nat

A Caravan book. For more information, visit www.caravanbooks.org

Set in Garamond and Stone Sans types by Binghamton Valley Composition.
Printed in the United States of America by Vail-Ballou Press.

Library of Congress Cataloging-in-Publication Data

Solove, Daniel J., 1972–
The future of reputation : gossip, rumor, and privacy on the Internet / Daniel J. Solove.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-300-12498-9 (cloth : alk. paper) 1. Privacy, Right of. 2. Internet—Law and legislation. 3. Reputation (Law) 4. Libel and slander. 5. Personality (Law) I. Title
K3264.C65S65 2007
342.08'58—dc22
2007013364

A catalogue record for this book is available from the British Library.

The paper in this book meets the guidelines for permanence and durability of the Committee on Production Guidelines for Book Longevity of the Council on Library Resources.

10 9 8 7 6 5 4 3 2 1

Contents

Preface vii

1 Introduction: When Poop Goes Primetime, 1

Part I **Rumor and Reputation in a Digital World**

2 How the Free Flow of Information Liberates and Constrains Us, 17

3 Gossip and the Virtues of Knowing Less, 50

4 Shaming and the Digital Scarlet Letter, 76

Part II **Privacy, Free Speech, and the Law**

5 The Role of Law, 105

6 Free Speech, Anonymity, and Accountability, 125

7 Privacy in an Overexposed World, 161

8 Conclusion: The Future of Reputation, 189

Notes 207

Index 237

This page intentionally left blank

Preface

The idea for this book came to me soon after I began blogging in May 2005. I found blogging to be enthralling and invigorating. I was fascinated by the thrill of expressing my thoughts to a broad audience yet acutely aware of how people could be hurt by gossip and rumors spreading over the Internet.

In an earlier book, *The Digital Person: Technology and Privacy in the Information Age,* I explored how businesses and the government were threatening privacy by collecting massive digital dossiers of information about people. In that book, it was easy to take sides. I argued that information collection and use were threatening people's freedom and well-being, and that greater protection of privacy was necessary. When it comes to gossip and rumor on the Internet, however, the culprit is ourselves. We're invading each other's privacy, and we're also even invading our own privacy by exposures of information we later come to regret. Individual rights are implicated on both sides of the equation. Protecting privacy can come into tension with safeguarding free speech, and I cherish both values. It is this conflict that animates this book.

Although I advance my own positions, my aim isn't to hold them out as end-all solutions. The purpose of the book is to explore in depth a set of fascinating yet very difficult questions and to propose some moderate compromises in the clash between privacy and free speech. There are no easy answers, but the issues are important, and I believe that it is essential that we wrestle with them.

Many people helped shape the ideas in this book through conversations and helpful comments on the manuscript: danah boyd, Bruce Boyden, Deven Desai, Tom Dienes, Howard Erichson, Henry Farrell, Bill Frucht, Eric Goldman, Marcia Hofmann, Chris Hoofnagle, Orin Kerr, Ray Ku, David Lat, Jennie Meade, Frank Pasquale, Neil Richards, Paul Schwartz, Michael Sullivan, Bob Tuttle, Christopher Wolf, and David Wolitz. My research assistants, James Murphy and Erica Ruddy, provided helpful research and proofreading. A few passages in this book were adapted from my article "The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure," 53 *Duke Law Journal* 967 (2003). My agent, Susan Schulman, believed in this book from the start and helped tremendously in bringing it to fruition. I would also like to thank Michael O'Malley at Yale University Press, who also believed in this project and gave me the opportunity to bring it to life, and Dan Heaton, for his thoughtful editing of the manuscript.

When quoting from blog posts, I have occasionally corrected obvious typos and spelling errors.

Chapter 7 Privacy in an Overexposed World

In our overexposed world, is anything private anymore? Currently, the law recognizes as private only information that is completely secret. Information exposed to others is public. Privacy, however, is far more complicated, as it involves a cluster of nuanced expectations of accessibility, confidentiality, and control. If we are to protect privacy today, we need to rethink our understandings of privacy. This chapter is about how to do so.

PRIVACY IN PUBLIC

The Burning Man Festival is held each year in the barrens of the Nevada desert. Tens of thousands of people converge on a vast dusty area far away from the urban world to engage in a spiritual celebration of "radical self-expression." People dance, frolic, parade, act out skits, paint their bodies, sing, and create art. There is a lot of nudity. The festival is named for its concluding ritual, in which a forty-foot effigy of a man is set on fire. The Burning Man Festival has been an annual event since 1986. At first, it drew fewer

than two dozen people, but it has now grown to more than twenty-five thousand.[1]

In 2002 a website called Voyeur Video began to sell a dozen videos of nude participants at the festival. The videos, priced at $29.95, were peddled along with other classics such as *Kinky Nude Beach Day* and *Springbreak Stripoffs*. Voyeur Video fashioned itself not as a pornography company but as "a news company that reports on adult parties where people get naked and naughty."[2]

At the Burning Man festival, participants were allowed to make videos and take pictures, but only with the permission of festival organizers. Voyeur Video sought and was denied permission to videotape the event.[3] The company videotaped the festival anyway. The organizers sued. Among the many causes of actions were the Warren and Brandeis torts of appropriation and public disclosure. Video Voyeur backed down. It agreed to stop selling the videos and to turn them over to the Burning Man organizers.

The Burning Man case, although never fully litigated, raises several important questions about the nature of privacy. If a person is naked at a festival with twenty-five thousand others, how can that person claim privacy? Should the law recognize such claims?

The Law's Binary Understanding of Privacy

A husband and wife were engaged in a romantic embrace near an ice cream stand at a farmer's market. Their photo was snapped, and it appeared in the October 1947 issue of *Harper's Bazaar* in an article celebrating the splendor of love. The photo was also published in the May 1949 issue of *Ladies' Home Journal*. Although the photo depicted the couple in a moment of love, the couple wasn't in love with the fact that their intimacy was displayed in national magazines, and they felt humiliated and embarrassed. They sued the magazines for publicly disclosing private facts.

But the court threw out their case because the couple "had voluntarily exposed themselves to public gaze in a pose open to the view of any persons who might then be at or near their place of business."[4] According to the court, "There can be no privacy in that which is already public." The court reasoned that "the photograph did not disclose anything which until then had been private, but rather only extended knowledge of the particular incident to a somewhat larger public then had actually witnessed it at the time of occurrence."

One judge dissented in the case. He noted that "there is no news or educational value whatsoever in the photograph alone" and that a picture with models could readily have been used to illustrate the story. The judge went on to argue:

> By plaintiffs doing what they did in view of a tiny fraction of the public, does not mean that they consented to observation by the millions of readers of the defendant's magazine. In effect, the majority holding means that anything anyone does outside of his own home is with consent to the publication thereof, because, under those circumstances he waives his right of privacy even though there is no news value in the event. If such were the case, the blameless exposure of a portion of the naked body of a man or woman in a public place as the result of inefficient buttons, hooks or other clothes-holding devices could be freely photographed and widely published with complete immunity.

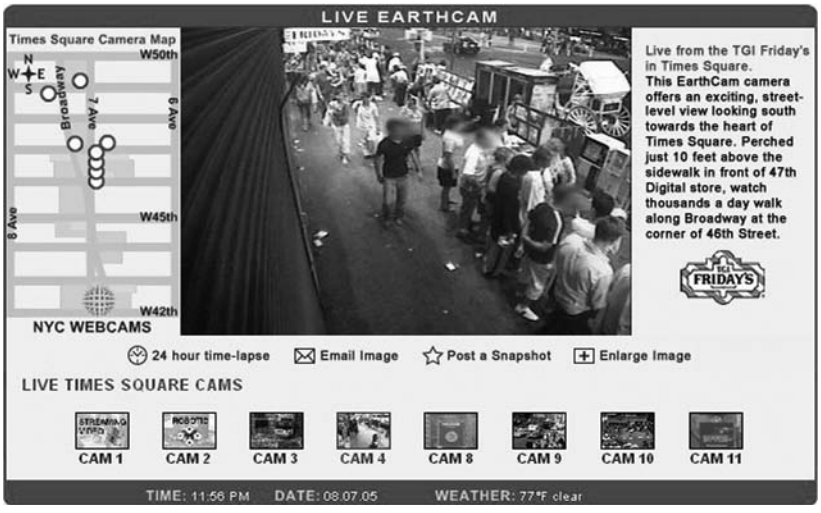
The judge has a point. There is a difference between what is captured in the fading memories of only a few people and what is broadcast to a worldwide audience. The law, however, generally holds that once something is exposed to the public, it can no longer be private. Traditionally privacy is viewed in a binary way, dividing the world into two distinct realms, the public and the private. If a person is in a public place, she cannot expect privacy. If information is exposed to the public in any way, it isn't private. According to the Restatement of Torts, one of the most influential documents for courts applying the tort of public disclosure: "There is no liability when the defendant merely gives further publicity to information about the plaintiff which is already public. Thus there is no liability for giving publicity to facts about the plaintiff's life which are matters of public record."[5] As one court ruled, appearing in public "necessarily involves doffing the cloak of privacy which the law protects."[6]

In one case, a husband and wife were arrested in a bar and taken away in handcuffs. A television film crew filmed the arrest. It turned out that the arrest was based on mistaken identity. The couple called the television station and begged that the footage not be broadcast. No such luck. The footage was aired. The couple sued, but the court dismissed the case because the arrest was filmed in public and was "left open to the public eye."[7]

Thus, according to the prevailing view of the law, if you're in public, you're exposing what you're doing to others, and it can't be private. If you really want privacy, you must take refuge in your home.

The Challenge of New Technology

Modern technology poses a severe challenge to the traditional binary understanding of privacy. Today data is gathered about us at every turn. Surveillance cameras are sprouting up everywhere. There are twenty-four-hour surveillance cameras in public linked to websites for anybody to view. Go to EarthCam and click on one of many major cities, such as Washington, D.C.,



The EarthCam website, displaying a feed from its live Times Square camera. Image courtesy of EarthCam, Inc.

Chicago, New York, or Seattle, among others.[8] In New York, for example, you can watch a camera that captures people walking down the sidewalk at 47th Street in Times Square.

Armed with cell phone cameras, everyday people can snap up images, becoming amateur paparazzi. Websites like Flickr allow people to post their photos and share them with the world.[9] Some people are posting a daily stream of photos, obsessively documenting every aspect of their lives. Beyond pictures, people are posting videos on the Internet for the world to watch. On YouTube, the leading video website, people around the globe are viewing more than one hundred million videos per day. On a daily basis, people add more than sixty-five thousand videos to YouTube.[10] Other variations of blogs are emerging, ones devoted primarily to pictures and video. A "moblog" is short for "mobile weblog."[11] Moblogs consist of postings based on what people capture in their mobile devices, such as cell phone cameras. Video blogs, or "vlogs" for short, consist of video feeds. According to one vlogger, everyone can "create media and have a distribution outlet for it that bypasses television and mainstream media."[12]

Today, privacy goes far beyond whether something is exposed to others. What matters most is the nature of the exposure and what is done with the information. There is a difference between casual observation and the more in-

delible recording of information and images. As the law professor Andrew McClurg points out, captured images have permanence, something fleeting memories lack. People can scrutinize a photo and notice details that they might not otherwise see when observing the scene as it unfolds.[13]

A second difference involves the degree of anonymity we expect in our everyday activities. As one prescient judge wrote, privacy can be "invaded through extensive or exhaustive monitoring and cataloguing of acts normally disconnected and anonymous."[14] We often engage in our daily activities in public expecting to be just a face in the crowd, another ant in the colony. We run into hundreds of strangers every day and don't expect them to know who we are or to care about what we do. We don't expect the clerk at the store to take an interest in what we buy. In other words, we're relatively anonymous in a large part of our lives in public. Identification dramatically alters the equation.

Suppose somebody followed you around in a drug store. The person assiduously scribbled down an inventory of what you bought. Or the person snapped a photo of the products you had in your basket as you were waiting at the checkout counter. Perhaps you wouldn't want the world to know you had bought hemorrhoid cream. Or perhaps you wouldn't be thrilled that others would know about your diarrhea problem or the kind of birth control you used. You bought all these things in public, and you exposed them to other people. Does this mean that you don't expect privacy in what you bought?

A third component of our expectations involves our understanding of context. Although we do things in public, we do them in a particular context before a particular set of people. As the information technology scholar Helen Nissenbaum points out, "it is crucial to know the context—who is gathering the information, who is analyzing it, who is disseminating it and to whom, the nature of the information, the relationships among the various parties, and even larger institutional and social circumstances."[15] McClurg aptly notes that "a photograph permits dissemination of an image not just to a larger audience, but to different audiences than the subject intended." Moreover, "conduct which would be appropriate for one environment may be inappropriate or embarrassing in another."[16] We tell jokes to our friends we wouldn't tell to our grandmother. We realize that there are different social norms for different situations, and broadcasting matters beyond their original context takes away our ability to judge the situation appropriately.

Fourth, much of our daily lives occurs in realms that are neither purely

public nor purely private. Instead, our activities often take place in the twilight between public and private. We used to speak on the phone at home or in closed phone booths, but with cell phones, we now carry out our conversations in a variety of public places. Suppose you're on a train and you have a cell phone conversation with a friend. The person sitting next to you secretly records your conversation and makes the recording available online. Despite the fact you exposed your conversation to people nearby, you didn't expect your conversation to be recorded and made available to the world.

Most of us have moments when we're in public where we would not want a photo taken of us, much less placed on the Internet. Most of us have times when we expose personal information to others but do not expect it to be shared more widely. We frequently have conversations in public that we don't expect to be overheard. When we chat in a restaurant, we don't expect others to be straining to eavesdrop on our discussion above the din of other dinner conversations. At most, we might expect one or two people to hear fragments of what we're saying, but we certainly don't expect to see a transcript of our conversation appear on the Internet.

Thus merely assessing whether information is exposed in public or to others can no longer be adequate to determining whether we should protect it as private. Unless we rethink the binary notion of privacy, new technologies will increasingly invade the enclaves of privacy we enjoy in public. Privacy is a complicated set of norms, expectations, and desires that goes far beyond the simplistic notion that if you're in public, you have no privacy.

Video Voyeurism

In some instances, the law is beginning to advance beyond the simplistic binary view of privacy. The rise of video voyeurism has pushed the law toward a greater recognition of different degrees of privacy. New technology has made video voyeurism easy. Anybody armed with a cell phone camera can quickly snap photos of others in the buff and post them online. In one incident, nude photos of a men's wrestling team at the University of Pennsylvania appeared on a website. One athlete said: "I pulled up the home page and I am looking at myself naked on the Internet. . . . It is terrible because I have no control over it."[17]

Another practice is the taking of "upskirt" photos—pictures taken up women's skirts. More than one hundred websites are devoted to providing upskirt photos or pictures of people showering or undressing.[18] To take these photos, all a person needs is a cell phone camera.

Several states have responded by passing laws with criminal penalties for video voyeurism.[19] Some initial attempts at creating these laws, however, failed because of the binary view of privacy. In one case, two men took upskirt photos of unsuspecting women in a mall. Both were convicted under a Washington video voyeurism statute. The Washington law defined the crime as taking photos "for the purpose of arousing or gratifying the sexual desire of any person" when the photo was taken "in a place where [the victim] would have a reasonable expectation of privacy."[20] The Washington Supreme Court, however, overturned the conviction because "although the Legislature may have intended to cover intrusions of privacy in public places, the plain language of the statute does not accomplish this goal." The court reasoned that "casual surveillance frequently occurs in public. Therefore, public places could not logically constitute locations where a person could reasonably expect to be safe from casual or hostile intrusion or surveillance."[21] The law was later amended to include both public and private places.

In 2004 Congress enacted the Video Voyeurism Prevention Act.[22] Congress criminalized video voyeurism, and it heeded the lesson from the Washington law, explicitly providing that the act would apply "regardless of whether [the victim] is in a public or private area." Unfortunately, Congress's act applies only on federal property, so you're safe from upskirt photos if you're walking in the Capitol Building or on other federal property. But if you're in the local mall, then you better hope that your state has a video voyeurism law, and if it does, that it has made clear that you can expect some level of privacy in public. The example of video voyeurism demonstrates that privacy expectations do not turn solely on place.

Many places aren't purely private or purely public. Suppose you're in a gym locker room and somebody snaps a photo of you undressing and posts it online. Is the locker room a public or a private place? It isn't entirely private, since it is open to other people, and you're undressing in front of many others. But although you're not in seclusion, you can expect that others won't take photos of you. Restrooms, stores, bars, and other places are open to the public, but this doesn't eliminate your expectations of privacy in those places. Expectations of privacy turn on norms. You expect privacy in the gym locker room because the norms are clear that it is inappropriate for others to snap your photo in this context. And in the Nevada desert, the participants of Burning Man have established a set of norms about how others are to use photos.

So we're back to the Burning Man festival. The Burning Man case illus-

trates that a claim of privacy is not the same as a claim of absolute secrecy. The participants of Burning Man obviously didn't mind being seen nude by other participants. They didn't even mind having their photos taken by others. What they didn't want was their images being exploited by pornographers. All-or-nothing notions of privacy fail to grasp the central difference between fellow festival goers and commercial exploiters for porn. There's a mutual camaraderie among festival goers that isn't shared with the pornographers. The Burning Man participants thus had nuanced expectations of privacy—about how their information would be used within a limited circle of people.

The Difficulties of Recognizing Privacy in Public

The law should begin to recognize some degree of privacy in public. But there are difficulties with doing so. Suppose you witness an interesting event on the subway and you want to capture it on your cell phone camera to post on your blog. If the people you were photographing on the subway had privacy rights in public, you might need their permission to post the photo. And if they are engaging in a social taboo, they might not be eager to give you permission. Should you be allowed to post the picture anyway?

The abstract hypothetical I suggest above can apply to a number of situations already discussed in this book—the dog poop girl and the New York City subway flasher. One might ask incredulously: So the dog poop girl engages in a nasty transgression and the law will stop people from taking her picture and exposing her misbehavior? Should the law give the creep who flashes on the subway a right to sue a person who took a photo of him in the act? These are potential implications of a robust recognition of privacy in public. The law need not go this far, but is there a logical stopping point? I've discussed some of the problems with online shaming, so perhaps protecting the dog poop girl or the subway flasher has significant benefits in curtailing the abuse of shaming. One might argue that only people engaged in illegal activities or severe norm violations lack privacy, but who is to judge this? The average person with a cell phone camera? It is difficult to stop shaming unless we protect privacy in public. Doing so doesn't mean absolute protection, just a limit on certain kinds of uses and disclosures. People can still snap pictures and turn them over to the police. People should be deterred, however, from taking matters into their own hands by placing the photos online.

When the law begins to recognize privacy in public, the tricky question is:

How much? Would streakers in Times Square still have the right to claim privacy if people posted their photos on the Internet? At some point, what is done in public is indeed public. There are no easy answers, and the resolution will depend upon the norms and expectations in each circumstance. The virtue of the binary view of privacy is clarity. It is an easy rule to apply. Yet the simplicity of this view is its downfall—it seems far too outmoded given new technology. Therefore, although it will be difficult, it is better to develop and protect a more nuanced notion of privacy.

Accessibility of Information

In 2006 Facebook (a social network website consisting of millions of high school and college students) launched a feature called News Feed that instantly alerted users whenever their friends added information or photos to their profiles. Facebook users constantly update their profiles, adding new text and new images. They might update their roster of friends. The News Feed feature immediately notified all of a person's friends about each new change in that person's profile.

News Feed was met by an enormous outcry from users, who vociferously objected to the extensiveness of the exposure. According to one of the users, "Facebook is becoming the Big Brother of the Internet recording every single move."[23] "It's just so unnecessary," another user complained. "You don't have to know everything your friends do and the changes they make. . . . It's kind of creepy."[24] As one user expounded: "Before News Feed, yes, you could see the profile, and you could see the pictures, and you could see the comments, and you could see the relationship status, but the users felt that it was just for people who cared, and who wanted to know. But now, all of this information was thrown down the throats of everyone, and it was very strange."[25] Shortly after the change, a protest group called "Students Against Facebook News Feeds" emerged on Facebook.[26] People joined the group in droves. Within days, the number of protesters had swelled to more than seven hundred thousand.[27]

Facebook quickly responded. Mark Zuckerberg, the creator of Facebook, wrote an open letter to Facebook users: "We really messed this one up. When we launched News Feed and Mini-Feed we were trying to provide you with a stream of information about your social world. Instead, we did a bad job of explaining what the news features were and an even worse job of giving you control of them. I'd like to try to correct those errors now."[28]

The Facebook privacy debacle is especially interesting because it had nothing to do with the exposure of new information. No new secrets about Face-

book users were being revealed. The information that the users complained about was already available on their profiles—posted voluntarily by themselves. Instead, all the new system did was alert users to that new information. In other words, the Facebook system was merely making existing information more accessible. Perhaps this explains why Facebook officials were so surprised by the backlash. After all, Facebook users are not a bunch who seem very concerned about their privacy. Why, then, was there such a vehement reaction?

The Facebook change brought users an increased awareness of the privacy dangers of the Internet. Although Facebook users might think it is too quaint to expect all of their secrets to remain in the bag, this doesn't mean that they don't care about privacy. They just see privacy differently. What many of the Facebook users objected to was the increased accessibility of their personal data—the fact that others would be alerted to every new update to their profiles immediately. Privacy can be violated not just by revealing previously concealed secrets, but by increasing the accessibility to information already available. The desire for privacy is thus much more granular than the current binary model recognizes. Privacy involves degrees, not absolutes. It involves establishing control over personal information, not merely keeping it completely secret. As the computer security expert Bruce Schneier argues: "People are willing to share all sorts of information as long as they are in control. When Facebook unilaterally changed the rules about how personal information was revealed, it reminded people that they weren't in control."[29]

For example, suppose you had a spat with a friend and wanted to eliminate that person from your circle of friends on Facebook. You might not want this change to be announced prominently to all your other friends. You might want the change to be made quietly, where it might be noticed by a few friends, or by no one besides you and the former friend. In other words, you might want some changes to fly under the radar. The binary view of privacy doesn't recognize the wide swath of middle ground between the realms of absolutely public and absolutely private. Increasingly, however, our lives occupy this middle ground. That's why I believe we must abandon the binary view of privacy and develop a more nuanced view.

CONFIDENTIALITY

Aleksey was an ambitious twenty-three-year-old student at Yale University. Desiring to be an investment banker, he applied to UBS, a global financial

company. His application, however, was rather unusual. First of all, his résumé was rather long—eleven pages in all. Even more peculiarly, he sent along a seven-minute video of himself entitled "Impossible Is Nothing."

The video begins with Aleksey being interviewed as if he were a famous individual. The interviewer calls Aleksey a "model of personal development and inspiration to many around you," then asks, "How do some people like yourself become very proficient in their fields faster than most?" "Well, thank you," Aleksey replies. "I guess the first thing people need to understand is that success is a mental transformation; it is not an external event."

Throughout the video, with an aloof and serious tone, Aleksey pontificates about his philosophy of success. "Ignore the losers," Aleksey says, "bring your A-game, your determination and your drive to the field, and success will follow you." In other pearls of advice, Aleksey declares that "failure cannot be considered an option," and that "luck doesn't jump into anyone's lap."

The video frequently cuts to scenes demonstrating Aleksey's athletic prowess. He performs a series of rather unusual skills for an investment banker position. Aleksey lifts massive dumbbells, bench presses 495 pounds, serves a 140-mph tennis ball, does an acrobatic ski jump, and concludes by breaking a stack of bricks with a karate chop.

"If you're going to work, work," Aleksey declares. "If you're going to train, train. If you're going to dance, then dance, but do it with passion." The video then cuts to Aleksey dancing with a scantily clad woman to Chayanne's "Solamente Tu Amor." The video concludes with Hans Zimmer's "The Way of the Sword" playing over end credits.

Needless to say, Aleksey wasn't hired by UBS. But his video was forwarded around Wall Street, and it soon wound up on YouTube. In a short time, hundreds of thousands of people had downloaded it. Aleksey sent requests to websites to take the video down, but in vain.[30] Aleksey had become an Internet sensation. One media website in the United Kingdom declared Aleksey's video the "greatest CV ever filmed."[31] The mainstream media pounced on the story. The *New York Post* called his video a "six-minute ego-mercial."[32] An article in the *New York Times* declared that Aleksey "may be the most famous investment-banking job applicant in recent memory."[33] Throughout the blogosphere, people accused Aleksey of being a pathological liar, of faking the feats in the video, and of plagiarizing in a book he had self-published. At DealBook, a blog sponsored by the *New York Times,*[34] commentators to a post by journalist Andrew Sorkin declared:

> That kid should be stripped of his degree. It seems reasonably clear that he has lived a life of lies.
>
> Another victim of a self-absorbed, dishonest and Idol-worshipping American culture.
>
> What an insufferable, self-absorbed, arrogant and self-aggrandizing jerk. In other words, a perfect fit for Wall Street.

Aleksey appeared on television media shows to respond to his worldwide mockery. On MSNBC, Aleksey stated in an interview that he was shocked to see his video and résumé spread across the Internet. His résumé contained his phone number and email address, and he was receiving harassing cell phone calls and thousands of nasty emails.[35] At Harvard students threw an Aleksey theme party, with people dressing up in karate uniforms and dancing attire.[36] The blog Gawker anointed Aleksey with the title of "pioneer Douchebag."[37] In an interview on ABC's *20/20,* Aleksey stated that he thought he had no chance now for a career on Wall Street. "So far," he said, "it's been like going through hell."[38]

Did Aleksey get what he deserved? Perhaps such a pompous person should be put in his place. But at what cost? On Sorkin's DealBook post, other commentators questioned whether it was appropriate for Aleksey's résumé and video to be leaked on the Internet:

> I am deeply disturbed [that] a resume sent in confidence to a highly respected firm had been made public and that confidence [was] broken. Should we all worry about where [our resumes] end up once sent to the firm of our choice?
>
> Although the kid is obviously a ridiculous egomaniac and not a particularly good liar, the real guilty party here is UBS.
>
> This fellow is being subjected (in Clarence Thomas' immortal words) to a "high-tech lynching." Whether or not he embellished or misrepresented anything in his job app or his resume or anything else in his life, it's beyond the pale to have the entire snarky Internet . . . pile on him in public.

In all fairness to UBS, the precise story of how the video and resume got leaked is unclear. UBS issued a statement about the matter: "As a firm, UBS obviously respects the privacy of applicants' correspondence and does not circulate job applications and resumes to the public. To the extent that any policy was breached, it will be dealt with appropriately."[39]

Assuming Aleksey's application was leaked by somebody at UBS, is the application really private? One could argue that Aleksey's application was no longer private after he sent it to UBS. However, there is a significant difference between a few employees at UBS having a chuckle over Aleksey's application and the entire world making Aleksey the butt of their jokes. Although the video wasn't completely secret since Aleksey exposed it to some people at UBS, the general public wasn't Aleksey's intended audience. Should the law respect Aleksey's desire to expose his personal information selectively? Or since he revealed his information to others, can he continue to claim that it is private?

Should We Assume the Risk of Betrayal?

Suppose your spurned ex-lover decides to post the intimate details of your relationship online. Or imagine that a trusted friend reveals your deepest secrets on her blog. This is increasingly happening online. Jessica Cutler's Washingtonienne blog is a prime example. The private information about people on the Internet often doesn't come from strangers but from friends, family members, coworkers, and others.

If you tell something to your doctor, you expect her to keep it confidential. It's an unwritten expectation, something that is rarely explicitly said but that is generally understood. Indeed, doctors are under ethical obligations to keep patient information confidential. People don't expect their doctor to be blogging about them on the sly.

Confidentiality differs substantially from secrecy. Secrecy involves hiding information, concealing it from others. Secrecy entails expectations that the skeletons in one's closet will remain shut away in the darkness. In contrast, confidentiality involves sharing one's secrets with select others. Confidentiality is an expectation within a relationship. When we tell others intimate information, we expect them to keep it confidential. Sharing personal data with others makes us vulnerable. We must trust others not to betray us by leaking our information.

The importance of confidentiality has been recognized since antiquity. Ethical rules have long existed for physicians to maintain the confidentiality of their patients' information. The Hippocratic Oath, circa 400 B.C., provides that doctors "will keep silence" about what their patients tell them.[40] Confidentiality is essential for certain communications to take place. Mark Twain explained most vividly why confidentiality is so important: "The frankest and freest and privatest product of the human mind and heart is a love letter; the

writer gets his limitless freedom of statement and expression from his sense that no stranger is going to see what he is writing. Sometimes there is a breach-of-promise case by and by; and when he sees his letter in print it makes him cruelly uncomfortable and he perceives that he never would have unbosomed himself to that large and honest degree if he had known that he was writing for the public."[41]

American law currently plays Jekyll and Hyde with regard to protecting confidentiality. Sometimes, the law strongly protects confidentiality. For example, the law provides potent protections for patient-physician confidentiality. As one court put it: "There can be no reticence, no reservation, no reluctance when patients discuss their problems with their doctors."[42] The law protects the confidentiality of people's discussions with their attorneys to "encourage full and frank communication."[43] The law also protects marital communications between spouses, a protection that dates as far back as ancient Jewish and Roman law.[44]

But in many cases, the law turns a blind eye to breaches of confidentiality, holding that we must assume the risk that we'll be betrayed. Most courts have not protected communications between parents and children.[45] As a result, parents and children can be forced to testify against each other in court.[46] In criticizing this doctrine, one court declared: "Forcing a mother and father to reveal their child's alleged misdeeds . . . is shocking to our sense of decency, fairness, or propriety."[47]

The law often holds that if you share a secret with others, you assume the risk that they will betray you.[48] In one case from 1970, for example, General Motors began a campaign to dig up dirt on Ralph Nader, who had been criticizing the safety of GM's cars. Among other things, GM sent people to find out Nader's secrets by talking with his friends and acquaintances. GM also made harassing phone calls, wiretapped his telephone, and kept him under extensive surveillance when in public. Although the court held that some of GM's tactics were improper, it concluded that there was nothing wrong with trying to get Nader's friends to betray his secrets. If a person shares information with another, the court declared, "he would necessarily assume the risk that a friend or acquaintance in whom he had confided might breach the confidence."[49] Although the law protects spouses from having to testify against each other, it often does not provide a remedy when one spouse (or ex-spouse) writes a tell-all book about the other.

In contrast, the law in England strongly protects against betrayal of confi-

dence. People can be liable for disclosing secrets that are entrusted to them in confidence.[50] In one English case, a man who had a homosexual affair with the actor Michael Barrymore told the details to a reporter for the paper *The Sun*. The court protected Barrymore: "When people enter into a personal relationship of this nature, they do not do so for the purpose of it subsequently being published in *The Sun,* or any other newspaper. The information about the relationship is for the relationship and not for a wider purpose."[51] According to the court: "The fact is that when people kiss and later one of them tells, that second person is almost certainly breaking a confidential arrangement."[52]

In another English case, the actors Michael Douglas and Catherine Zeta-Jones made an exclusive deal with *OK!* magazine to publish the photos of their wedding. Guests were told that they weren't allowed to take photos. But not to be outdone, *Hello!* magazine had a photographer masquerade as a guest and secretly snap pictures. The court ruled that *Hello!* had engaged in a breach of confidence.[53]

The United States has a breach-of-confidentiality tort, although it is much weaker than the tort in England.[54] In the United States, the number of relationships understood to be confidential is small. Beyond doctors, lawyers, clergy, and a few others, the information you tell others is often not legally protected. You might trust a best friend with your secrets, but your friend can betray you without breaking the law. Boyfriends, girlfriends, family members, colleagues, and others are under little obligation to keep your information private.

Beyond those you trust the most with your information, you also routinely put your trust in people you barely know. For example, you expect the store clerk not to broadcast your purchases to the world. Day in, day out, we depend upon people keeping our information confidential. And yet these people are generally not understood to have a legal duty to do so.

The companies you share information with are also frequently not understood to owe you a legal duty of confidentiality. Unless you live in a shack in the woods, a significant amount of your most intimate information is shared in some way with others. Your ISP knows what websites you are visiting. Your phone company knows whom you're calling. Your credit card company knows how you're spending your money. Although we trust these companies with our personal information, the law only sometimes imposes upon them an obligation to keep it confidential.

Why is the American breach-of-confidentiality tort so much weaker than

the English version? One reason is that the breach-of-confidentiality tort became overshadowed by the other privacy torts. In their 1890 article that inspired the privacy torts, Warren and Brandeis were skeptical of the ability of confidentiality law to protect privacy. At the time, there was a rather robust law protecting confidential relationships. But Warren and Brandeis steered the law in a new direction. As we have seen, Warren and Brandeis had in mind the taking of candid photographs by strangers. In this situation, they noted, there was no confidential relationship. The law thus had to recognize a new protection of privacy, one that would provide remedies against strangers. Although Warren and Brandeis never explicitly rejected confidentiality, it was often overlooked by lawyers and judges who focused only on the other privacy torts instead.

The law should more expansively recognize duties of confidentiality. A large amount of the information about us that finds its way online isn't put there by strangers. It is spread by people's spurned lovers, their ex-spouses, their enemies, and in some cases, their friends. Perhaps we should recognize implicit promises of confidentiality when we share intimate information with others. You don't sign a confidentiality agreement with your doctor or lawyer before you start talking about your symptoms or your legal case. It's implied. We frequently expect confidentiality when we share intimate information. We place our trust in others to keep our secrets. So why not establish that when you tell somebody a secret, there's an implied promise that it's confidential? Although the tort of breach of confidentiality is not nearly as well developed as the tort in England, there is no reason why it can't evolve to provide stronger privacy protection.

Of course, there must be limits to how broadly the law should reach. People gossip all the time. As Benjamin Franklin once quipped, "Three may keep a secret if two are dead."[55] If the law became involved every time people gossiped, it would become far too entangled in our lives. Gossip is so frequent that we'd be constantly litigating. But the law should provide a remedy for gossip when it is spread widely or made permanent. As discussed earlier, Internet gossip is especially damaging. So the law can try to keep gossip off the Internet and confined to whispering tongues.

Social Network Theory

Not all information is confidential. Often the cat is already out of the bag. At that point, there are no obligations of confidentiality. But how do we know when the cat has escaped?

Rarely do we keep complete secrets. Indeed, when we tell someone a secret, we still call it a "secret" even though another person now knows it. Courts have a difficult time determining when a secret is no longer a secret. Suppose I tell it to one thousand people. Can I really claim it is a secret anymore? At some point, it's too late—my secret becomes public information.

In one case, Jane Doe came back to her apartment and saw the corpse of her murdered roommate lying on the floor. She also caught a glimpse of her roommate's killer as he fled.[56] Since the killer was still at large—and since Jane was an eyewitness, the police withheld her identity from the public. But somehow it got leaked to a journalist, who named her in a newspaper article about the murder. Jane sued under the public-disclosure tort. The newspaper argued that Jane's identity wasn't private because she told some of her neighbors, friends, and family members about witnessing the murder. Thus the secret was known to a few people. But the court wisely disagreed with the newspaper, concluding that Jane had not "rendered otherwise private information public by cooperating in the criminal investigation and seeking solace from friends and relatives."

In another case, a couple conceived using in vitro fertilization. Artificial means of conception were against the teachings of their religion, so the couple kept the information confidential from members of their congregation and local community. But employees at the hospital knew about their in vitro fertilization and so did other couples at the hospital undergoing similar procedures. On one occasion, a party was thrown for the in vitro couples. A television crew filmed the event, and despite the couple's best efforts to avoid being filmed, their images were nevertheless broadcast on television. The couple sued under the public-disclosure tort. The court held that the couple retained an expectation of privacy because "attending this limited gathering . . . did not waive their right to keep their condition and the process of in vitro private, in respect to the general public."[57]

In another incident, an HIV-positive individual told nearly sixty other people about his condition. They included family, friends, doctors, and members of an HIV support group. At one point, the person agreed to appear on a television show, but only with his face obscured. Unfortunately, the obscuring process was botched, and the individual was identifiable. He sued. The television company argued that he lost any expectation of privacy by telling so many people. But the court concluded that the individual still expected privacy because the people he told weren't likely to spread the information since they "cared about him . . . or because they also had AIDS."[58]

In all these cases, courts concluded that although people exposed their secrets to several others, they still could claim that the information was private. But many other courts have concluded otherwise. In one case a Colombian judge indicted Pablo Escobar, the infamous drug lord of Colombia. Escobar put a million dollar bounty on the judge's head. After receiving numerous death threats, she fled to Detroit. She told a few people there about her identity, but otherwise, she kept it quiet. The media, however, reported her story and revealed her address. She sued for public disclosure. The court threw out her case because she had exposed her identity "to the public eye."[59]

In another case, a woman told four coworkers about encounters with her child that had "sexual overtones." The court concluded that she no longer expected privacy in the information because she had shared it with four others in the office.[60]

How many people must know before the cat's out of the bag? Simply doing a head count of how many people know the information is the wrong approach. If something can remain private despite being known by four other people, why not five? Or ten? Or fifty? When is the exposure so great that we should say that the information is public and no longer private?

There is no magic number. Instead, as the law professor Lior Strahilevitz suggests, we should look to social networks.[61] As we have seen, people relate to each other in various groups or cliques. It is generally likely that our information will stay within the groups we associate with and not leave these boundaries. Instead of counting how many other people know certain information, we should focus on the social circles in which information travels. We all associate in various social circles. We have our groups of friends, the people where we work, our families. We share information within these groups. Rarely does gossip leap from one group to another. People in one social circle will often not know or care about a person in a completely different circle.

We're all separated by only a few links, but a degree of separation can be a chasm when it comes to the flow of gossip. As Strahilevitz notes, a "rural farmer in Omaha and a banker in Boston may be separated by only a few links, and yet they will live their entire lives oblivious to each other's existence." Suppose the farmer has a friend (Bob) who has a friend (Jane) who knows the banker. The farmer tells Bob about their mutual friend Jack's adulterous affair. Bob may tell Jane about it, but probably only if Jane knows Jack. Otherwise, why would Jane care? Strahilevitz observes that the information won't spread beyond the farmer's immediate social circle. Indeed, it probably won't even spread to the farmer's friends who don't know Jack, let alone

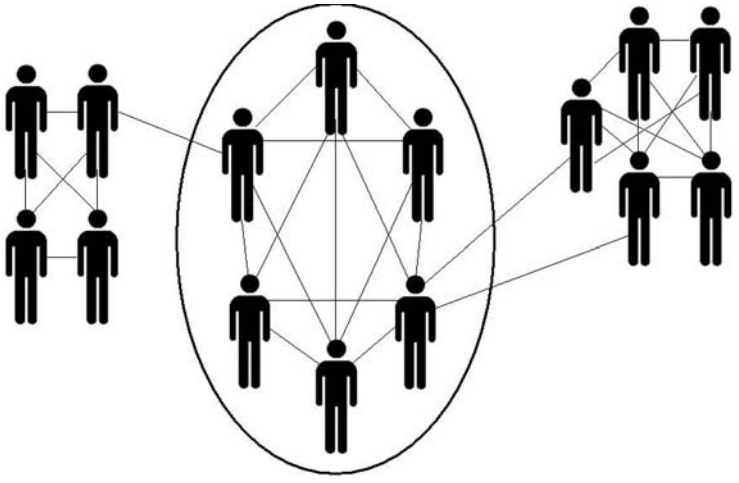
friends of friends. Only if the information is "particularly sordid, humorous, or memorable" will it spread further. If it does spread, those who don't know Jack will care only about the salacious details, not about his identity. Thus as the story radiates beyond those who know Jack, his name is likely to be dropped.

Social network theory often focuses primarily on connections, but networks involve more than nodes and links. There are norms about information sharing that are held within certain groups, such as norms of confidentiality. My colleagues at the law school where I teach constitute a social circle. Gossip travels quickly throughout the faculty, in part because we all work in the same building and encounter each other throughout the year. But while we might not be very careful about keeping secrets about our colleagues from our fellow colleagues, we're less likely to share gossip with students. Our relationships with students are more formal than our relationships with other colleagues, so gossip is not to be a likely topic of conversation. Many faculty might be wary of embarrassing a colleague by spreading rumors among the students. So despite close proximity between professors and students, despite many links between nodes, information might not spread evenly throughout a network because of norms.

In other words, certain groups guard secrets more tightly. Other times, secrets will not leave the group simply because outsiders won't be interested. The adage "What happens in Vegas stays in Vegas" aptly describes the phenomenon. What is gossiped about in certain groups often stays within those groups.

As Strahilevitz argues, we should examine how information is likely to travel. Information should be considered private if it remains within a confined group—even if that group is rather large. Once it has traversed too many social circles, then it is no longer private. But if the information is confined in a particular social circle, and a person takes it beyond these boundaries, that's when the law should assign liability—to the person who crossed the boundary.

According to Strahilevitz, the case in which the person's HIV status was still private despite being known to sixty others was correctly decided because the circles in which the person spread the information would readily respect the privacy of HIV-positive individuals. This isn't the kind of information that people typically spread about others, especially those who also suffer from the disease. Given these facts, Strahilevitz contends that the information was not likely to spread beyond the particular circle.



This diagram depicts three social groups in a network. The circle around the group in the center represents a boundary of information flow. Information circulating in the center group will rarely jump beyond that group even though some people in the group are linked to others in different groups.

Strahilevitz argues that the court was wrong, however, in the case involving the judge whose life was threatened by Pablo Escobar: "According to the court, [the woman] used her real name when shopping in stores or eating in restaurants, which waived an expectation of privacy in her identity. Under a network theory approach, these acts, combined with her notoriety in Colombia, would not have eliminated her reasonable expectation of privacy in her identity." The people she used her real name with were a few individuals she had "fleeting contact" with, such as people she encountered when shopping and at restaurants. These individuals were unlikely to care enough about who she was to spread news of her identity. Nor were they likely to "put two and two together" and realize that she was the woman with the bounty on her head. Her "general obscurity in Detroit properly engendered a reasonable expectation of privacy with respect to her shopping and visiting restaurants."[62]

Applying social network theory to the law of privacy doesn't require special expertise in sociology. We all have pretty good intuitions about how gossip travels. We readily understand that information can traverse quickly within certain groups but not spread beyond. It is this key intuition, one we know from experience and that is confirmed by social network theory, that privacy law needs to better understand and incorporate. When information is con-

tained within a particular group and a person causes it to leap the boundary, then this is a privacy violation even if the original group is large. So a big group of people can know a secret, and it can still be deemed private because it is not expected to circulate beyond that group.

From Realspace to the Internet

Even if information is already circulating orally as gossip among a few people, putting it online should still be understood as a violation of privacy—even if it is read only by people within one's social circle. In other words, a person might expose your secrets in her blog but defend herself by saying: "But only a few of my friends read my blog." The difficulty is that putting the information online increases dramatically the risk of exposure beyond one's social circle. Placing information on the Internet is not just an extension of water cooler gossip; it is a profoundly different kind of exposure, one that transforms gossip into a widespread and permanent stain on people's reputations.

There has been a long-standing recognition that written gossip can be more pernicious than oral gossip. In the late eighteenth century, for example, politicians frequently circulated gossip about each other. President Thomas Jefferson was a master at spreading gossip about his foes. Despite the crudeness of the practice, there was an "etiquette of gossip."[63] One of the primary rules was that gossip should never be put to pen, since letters and papers often found their way into the wrong hands, and even worse, could become exposed to the public. As the historian Joanne Freeman observes, written gossip was particularly dangerous because it could transform "one man's gossip into fodder for someone else's gossip."[64] Elites were careful about gossip; they understood its power and they tried to keep it in check as much as possible.

Today the line in the sand is the Internet. When gossip spreads to the Internet, it can spiral out of control. Even if it is posted on an obscure blog, information can still appear in a Google search under a person's name. Therefore the law should view the placing of information online as a violation of privacy—even gossip that had previously been circulating orally in one particular social circle.

How Far Should Liability Be Extended?

Social network theory explains why placing gossip on the Internet changes it so dramatically. The Internet allows information to traverse boundaries more rapidly and spread much farther. But when should liability end? Suppose that Jack posts private details about Jill's love life on his blog. Jack's blog has a

small readership. Marty, a blogger from a popular blog, with hundreds of thousands of readers, thinks that the story is interesting and posts excerpts of Jack's post. Who should be liable—Jack, Marty, or both?

Only Jack should be liable for damages. He's the one who breached the gossip boundary and spread the information to the Internet. Once the information is on the Internet, however, it would be impractical and problematic to hold liable others beyond the person who initially placed it there. A line must be drawn at cyberspace; once information is out on the Internet, those subsequently discussing and disseminating it should not be liable. To conclude otherwise would seriously chill the freewheeling and lively discussion that rapidly erupts across the blogosphere.

While this rule has its difficulties, it is the most practical approach. How is Marty to know how many others have read Jack's blog? At some point, liability must stop. When information is on the Internet, many people may readily link to it, talk about it, copy it, repost it, and so on. Putting gossip on the Internet is like throwing meat to alligators. People snap it up in a frenzy. Without protection from liability, people would be severely chilled in their blogging. They would never know when the information they have found on the Internet is really safe to blog about. Therefore only the person who first posts the gossip should be liable for damages. Those repeating the information should not be liable for damages—but they should be required to remove at least the last names of the harmed individuals if asked. If a reasonable request for suppression of personal information is denied, a victim should be able to seek legal recourse against bloggers and others who continue to broadcast identifiable information they find elsewhere on the Net.

The Danger of Too Much Confidentiality

One of the problems with confidentiality—and with privacy more generally—is that it impedes the spread of true information. If we protect confidentiality, we take away information that might be helpful in assessing people's reputations. In one example, a nurse was fired by a hospital for making serious errors. The nurse negotiated for the hospital to agree not to disclose any information about his performance on the job. The nurse then applied for a job at another hospital. That hospital sought a reference from the nurse's former place of employment. Despite promising confidentiality, the former hospital told the other one the reasons for firing the nurse. After a legal challenge, the court upheld the agreement as valid.[65] Was the former hospital in the wrong? Should it be liable for giving out an honest evaluation of the

nurse's performance? After all, it served the public interest by accurately providing information about a bad nurse whose errors could harm or kill future patients. It provided correct information that was helpful in assessing the nurse's qualifications. Confidentiality would have allowed the nurse to escape from his past. Should the law permit the withholding of such important information?

This case reveals the cost of confidentiality—sometimes the restriction of truth can cause harm to others. Hard cases exist, but most information on the Internet does not rise to this level. The law protects confidentiality even in some difficult cases because of the larger value of ensuring trust between people and encouraging candid conversations.

CONTROL

Dr. Laura Schlessinger hosted a popular national radio call-in show. She had conservative views, sternly espousing her moral judgments about sex, marriage, parenting, and abortion. She once declared that the best mothers are ones who stay at home, that being gay is a "biological error," and that women having sex outside marriage are "presenting themselves virtually as unpaid whores."[66] Dr. Laura, as she often has been called, published many books, including *Ten Stupid Things Women Do to Mess Up Their Lives, The Proper Care and Feeding of Husbands,* and *How Could You Do That?! The Abdication of Character, Courage, and Conscience,* among others.

In 1998 a website called Club Love posted about twelve photos of Schlessinger in the nude, taken about twenty-five years earlier when she was in her twenties. The website was run by Internet Entertainment Group, the same porn company that attempted to distribute a video of Pamela Anderson and Brett Michaels having sex.[67] The photos had been taken by Bill Ballance, who had introduced Schlessinger to radio back in 1974. Ballance had begun a brief affair with Schlessinger after she separated from her first husband, whom she later divorced. He kept the photos tucked away for years, then suddenly decided to sell them to Internet Entertainment Group.

One of the photos included a shot with Schlessinger in a spreadeagle pose. The website enabled people to click on any part of Schlessinger's anatomy and enlarge it for closer viewing. Internet Entertainment Group called the photos "The Dirty Dozen."[68] Soon after the photos were publicized, more than seventy other websites posted copies.[69]

Dr. Laura was distraught. She had strong words for Ballance: "I am mysti-

fied as to why, 23 years later, this 80-year-old man would do such a morally reprehensible thing."[70] She immediately sued and obtained a temporary restraining order against Internet Entertainment Group from posting the photos. But shortly afterward, the judge lifted the order on free-speech grounds. Before the case went any further, Dr. Laura dropped it.

Dr. Laura wasn't the only one upset. Internet Entertainment Group was also up in arms—against the other websites that it claimed were copying its photos. Copyright in a photo is owned initially by the person who takes the photo, not by the person whose photo is taken. When Ballance sold the photos, Internet Entertainment Group acquired the copyright. Seth Warshavsky, the head of Internet Entertainment Group, said: "We shut those sites down. We own the copyright to those photos and we intend to protect that copyright. If anyone, including Dr. Laura herself, tries to print those pix, we will shut them down."[71] That's right—Internet Entertainment Group's copyright even gives it the ability to control how Dr. Laura herself uses the photos.

While some might cheer this comeuppance of the harsh champion of family values, Internet Entertainment Group obtained the photos through Ballance's breach of confidentiality. It seems fairly clear that Schlessinger believed that the photos were to be kept by Ballance in confidence and not sold for profit. Copyright law gives Internet Entertainment Group a vigorous set of legal protections to control the use of the photos. The law gives Schlessinger much less control. Should the law be this way?

A System of Controlling Information

A problem with the binary view of privacy is that it is an all-or-nothing proposition. We often don't want absolute secrecy. Instead, we want to control how our information is used, to whom it is revealed, and how it is spread. We want to limit the flow of information, not stop it completely. Moreover, different people have different entitlements to know information about others. We might want to keep a person's HIV-positive status from her employer, but what about that person's spouse? Or people with whom the person had unprotected sex? In some cases, the law could say that some people should be entitled to know information but others shouldn't be.

But is control over information really feasible? If we expose information to others, isn't it too difficult for the law to allow us still to control it? Perhaps the law is reticent about granting control because of the practical difficulties. Information spreads rapidly, sometimes like a virus, and it is not easily contained. But in other contexts, the law has developed a robust system of con-

trolling information. For example, copyright law recognizes strong rights of control even though information is public. The Copyright Act protects "original works of authorship fixed in any tangible medium of expression."[72] Copyright law protects a wide range of works: movies, books, music, software, art, and photographs, among other things. To obtain copyright protection, one need not lock one's work behind closed doors. I expose copyrighted material to the public all the time. You're reading this book, which is copyrighted. My exposing the book to you doesn't eliminate my protection. You can't do whatever you want to with my book, such as photocopy it cover to cover and start selling bootleg copies in the streets of New York. But you can do some things with it. You can copy it for your own use. You can lend the book to others. You can quote from it. The copyright system focuses on the use of information—it allows certain uses and prohibits others. And it does so regardless of whether the information has been publicly exposed.

Moreover, copyright law provides protection even when a work can be readily copied. I don't have to take any steps to protect my work. Even if you can easily make copies and sell it, the law doesn't allow you to. In fact, the law even creates liability when others facilitate your violating my copyright protection. If you infringe upon my copyright, the law provides me with a powerful set of remedies. I can obtain a court order to forbid you from continuing to use my material improperly. I can sue for damages. Under certain circumstances you might also be subject to criminal penalties.

Copyright and privacy are both ways of controlling information. As the law professor Jonathan Zittrain notes, "there is a profound relationship between those who wish to protect intellectual property and those who wish to protect privacy."[73] The legal scholar Lawrence Lessig observes, "Just as the individual concerned about privacy wants to control who gets access to what and when, the copyright holder wants to control who gets access to what and when."[74] In privacy discussions, however, there seems to be a much lesser recognition of control. Control in the privacy context is seen as outlandish or impossible. Copyright law demonstrates otherwise. It reveals that the law is willing and able to control information.

Of course, copyright law isn't always effective at keeping information under control. People routinely violate copyright law, and as Zittrain notes, it is hard to control intellectual property when it can be so readily copied and transferred.[75] Despite these limitations, however, copyright law still has significant effects on the way information is disseminated and used.

I invoke copyright law not as a means to regulate privacy but merely to

demonstrate that the law can and does afford a vigorous system of control over information. With regard to privacy, the law needs better ways to allow people to exercise control over their personal data. I have discussed a few dimensions of such control already—a greater recognition of privacy in public and of duties to keep people's information confidential. The key question, of course, is how much control. Too much control over personal information can be just as bad as too little.

Copyright law's balance of freedom and control has been the subject of considerable debate and controversy. Several scholars, including Lessig, have criticized copyright law for providing too much control.[76] Copyright protections, for example, can impede me from creating works that use parts of others' works. For example, I might want to create my own *Star Wars* books and movies, using the characters George Lucas created, such as Darth Vader and Luke Skywalker. Copyright law bars me from doing this without Lucas's permission. Copyright's protections are so strong that even the First Amendment right to freedom of expression yields before them.[77] Copyright law's zealous protection of control over information can stifle creativity and free speech. In the context of privacy protection, the law need not foster the same level of control that copyright law affords. The key point is that the law is capable of providing a system for controlling information—even when information is not concealed from public view.

Refurbishing the Appropriation Tort

The closest privacy law comes to copyright is the appropriation tort. This tort, as described earlier, prevents the use of someone else's name or likeness for financial benefit.[78] Unfortunately, the tort has developed in a way that is often ineffective in protecting against the privacy threats we are facing today. Although the original rationale of the tort was to protect a person's privacy, the tort has in many cases been transformed into a kind of property right. Many of the successful cases involve celebrities whose identities have been used to endorse particular products without their consent. According to Jonathan Kahn, the "early association of appropriation claims with such intangible, non-commensurable attributes of the self as dignity and the integrity of one's persona seems to have been lost, or at least misplaced, as property-based conceptions of the legal status of identity have come to the fore."[79] An early 1905 case—the first state court to recognize the tort—explained the tort as protecting a person's freedom: "The body of a person cannot be put on exhibition at any time or at any place without his consent. The right of one to exhibit him-

self to the public at all proper times, in all proper places, and in a proper manner is embraced within the right of personal liberty. The right to withdraw from the public gaze at such times as a person may see fit, when his presence in public is not demanded by any rule of law, is also embraced within the right of personal liberty."[80] The court declared that the use of a person's identity against his will was akin to seizing his liberty, making him temporarily "under the control of another," with the effect "that he is no longer free, and that he is in reality a slave."[81]

But this meaning of the tort gradually became lost over the years. By 1960 the renowned torts scholar William Prosser explained that the injury redressed by the appropriation tort was "not so much a mental one as a proprietary one."[82] Thus appropriation used to focus primarily on protecting people's dignity, but now it centers around the profit-value of one's identity. We want to control information, however, not just to profit from it.

The appropriation tort is often limited to instances in which a person's identity is exploited for commercial gain. The tort doesn't apply when people's names or likenesses are used in news, art, literature, and so on. As one court noted, the tort doesn't apply to "factual, educational and historical data, or even entertainment and amusement concerning interesting phases of human activity."[83] The appropriation tort thus protects against my using your name or picture to advertise my products, but it allows me to use your name and picture when writing about you. I can write your unauthorized biography, for example, and you will not be able to sue me for appropriation.[84] I can use your picture in a news story about you. This limitation is a fairly big one. The appropriation tort would rarely apply to the discussion on the Internet of people's private lives or the posting of their photos.

The appropriation tort might be expanded to encompass a broader set of problematic uses of information about a person, but such an expansion would have to address some difficult issues. How much control do we want to give people over their images? An approach consistent with the newsworthiness test of the public disclosure tort would counsel that the appropriation tort apply when people's photos are used in ways that are not of public concern.

IS PRIVACY LAW UP TO THE TASK?

In this chapter, I've proposed that American privacy law adopt more nuanced understandings of privacy. Privacy law should recognize privacy in public; and it should better protect confidentiality. More generally, the law should al-

low individuals to exercise greater control over their personal information, even after it has been exposed to the public or to other people.

But are my recommendations too radical for our law? After all, law develops rather conservatively. It wears a bow tie, and it doesn't like change. Nevertheless, little by little, the law does evolve. The concepts discussed in this chapter—privacy in public, confidentiality, and control—are already present in American law, as well as in the law of many other countries. The law is beginning to recognize privacy in public places. A tort for breach of confidentiality exists in many countries—England, Australia, New Zealand, Canada, and others.[85] The tort exists in America, too, but it has not yet blossomed to its fullest potential. And the law recognizes the concept of control over information rather robustly in other contexts—perhaps too much in the copyright context. Thus there is plenty of legal precedent for privacy law to recognize more nuanced understandings of privacy. The seed certainly exists; the question is whether we'll let privacy law grow to respond to the new challenges we face.

Notes

CHAPTER 7. PRIVACY IN AN OVEREXPOSED WORLD

1. Jerome Burdi, *Burning Man Gets Hot over Steamy Videos,* Court TV, Aug. 26, 2002, http://archives.cnn.com/2002/LAW/08/26/ctv.burning.man/.
2. Evelyn Nieves, *A Festival with Nudity Sues a Sex Web Site,* N.Y. Times, July 5, 2002. Burning Man's suit was filed before the Video Voyeurism Prevention Act was introduced. Among the claims were intrusion, appropriation, public disclosure, breach of contract, and trespass.
3. *Id.*
4. Gill v. Hearst Pub. Co., 253 P.2d 441 (Cal. 1953).
5. Restatement (Second) of Torts §652D (comment c).
6. Cefalu v. Globe Newspaper Co., 391 N.E.2d 935, 939 (Mass. App. 1979).
7. Penwell v. Taft Broadcasting, 469 N.E.2d 1025 (Ohio App. 1984).
8. http://www.earthcam.com/.
9. http://flickr.com/.
10. *YouTube Serves Up 100 Million Videos a Day Online,* Reuters, July 16, 2006.
11. http://en.wikipedia.org/wiki/Moblog.
12. Katie Dean, *Blogging + Video = Vlogging,* Wired.com, July 13, 2005, http://www.wired.com/news/digiwood/0,1412,68171,00.html.
13. Andrew Jay McClurg, *Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places,* 73 N.C. L. Rev. 989, 1041–42 (1995).
14. Nader v. General Motors Corp., 255 N.E.2d 765, 772 (N.Y. App. 1970) (Brietel, J. concurring).
15. Helen Nissenbaum, *Privacy as Contextual Integrity,* 79 Wash. L. Rev. 119, 144–45 (2004).
16. McClurg, *Privacy Law, supra,* at 1041–43.
17. Marcia Chambers, *Colleges: Secret Videotapes Unnerve Athletes,* N.Y. Times, Aug. 9, 1999, at D4.
18. Clay Calvert, Voyeur Nation: Media, Privacy, and Peering in Modern Culture (2000).
19. *See, e.g.,* La. Rev. Stat. Ann. §14:283; N.J. Stat. Ann. §2C:18-3; N.Y. Penal Law §250.45.
20. RCW 9A.44.115.

21. Washington v. Glas, 54 P.3d 147 (Wash. 2002)
22. 18 U.S.C. §1801.
23. Quoted in Anick Jesdanun, *Facebook Feature Draws Privacy Conerns,* Associated Press, Sept. 7, 2006.
24. Dave Wischnowsky, *Facebook Alienates Users,* Chicago Tribune, Sept. 8, 2006.
25. Peter Meredith, *Facebook and the Politics of Privacy,* Mother Jones, Sept. 14, 2006.
26. Quoted in Jesdanun, *Facebook Feature, supra.*
27. Wischnowsky, *Facebook Alienates Users, supra.*
28. Mark Zuckerberg, *An Open Letter from Mark Zuckerberg: Creator of Facebook,* Sept. 8, 2006. The letter appeared on the Facebook website when users logged in. It has since been removed.
29. Bruce Schneier, *Lessons from the Facebook Riots,* Wired, Sept. 21, 2006.
30. Lisa Lerer, *How Not to Get a Job,* Forbes, Oct. 13, 2006.
31. *The Greatest CV Ever Filmed,* Oct. 10, 2006, http://www.metro.co.uk/weird/article.html?in_article_id=20878&in_page_id=2&expand rue.
32. Paul Tharp, *Wannabe Banker's Video Resume Backfires,* N.Y. Post, Oct. 12, 2006.
33. Michael J. de la Merced, *A Student's Video Résumé Gets Attention (Some of It Unwanted),* N.Y. Times, Oct. 21, 2006.
34. Comments to Andrew Ross Sorkin, *The Resume Mocked Around the World,* DealBook, Oct. 19, 2006, http://dealbook.blogs.nytimes.com/2006/10/19/the-resume-mocked-round-the-world-vayner-speaks/.
35. Interview with Aleksey, Rita Cosby Live, MSNBC, Oct. 23, 2006.
36. *Creepy Orwellian Trance of Aleksey Vayner Fails to Generate Fun,* IvyGate Blog, Nov. 20, 2006, http://ivygateblog.com/blog/2006/11/creepy_orwellian_trance_of_aleksey_vayner_fails_to_translate_into_fun.html.
37. *Douchebag Hall of Fame: The Inevitable Charter Member,* Gawker, Oct. 16, 2006, http://www.gawker.com/news/douchebag-hall-of-fame/douchebag-hall-of-fame-the-inevitable-charter-member-207845.php.
38. Interview with Aleksey on ABC, *20/20,* Dec. 29, 2006.
39. Merced, *Student's Video Résumé, supra.*
40. "Whatsoever things I see or hear concerning the life of men, in my attendance on the sick or even apart therefrom, which ought not to be noised abroad, I will keep silence thereon, counting such things to be as sacred secrets." Hippocratic Oath, quoted in Daniel J. Solove, Marc Rotenberg & Paul M. Schwartz, Information Privacy Law 350 (2d ed. 2006).
41. Mark Twain, The Autobiography of Mark Twain xxxv (Charles Neider, ed.).
42. Hammonds v. AETNA Casualty & Surety Co., 243 F. Supp. 793, 801 (D. Ohio 1965).
43. Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).
44. Wendy Meredith Watts, *The Parent-Child Privileges: Hardly a New or Revolutionary Concept,* 28 Wm. & Mary L. Rev. 583, 592 (1987); Glen Weissenberger, Federal Evidence §501.6, at 205–9 (1996).
45. In re Grand Jury, 103 F.3d 1140, 1146 (3d Cir. 1997) ("The overwhelming majority of all courts—federal and state—have rejected such a privilege.").
46. *See, e.g.,* State v. DeLong, 456 A.2d 877 (Me. 1983) (refusal to testify against father); Port

v. Heard, 594 F. Supp. 1212 (S.D. Tex. 1984) (refusal to testify against son); United States v. Jones, 683 F.2d 817 (4th Cir. 1982) (refusal to testify against father in grand jury).

47. In re A&M, 61 A.2d 426 (N.Y. 1978).
48. The Supreme Court has held that in Fourth Amendment law, people lack a reasonable expectation of privacy when they trust others with their information. *See, e.g.,* Smith v. Maryland, 442 U.S. 735, 744 (1979) (a person "assumes the risk that the [phone] company [will] reveal to the police the numbers he dialed."). Undercover agents are not regulated by the Fourth Amendment because people assume the risk of betrayal. *See* Hoffa v. United States, 385 U.S. 293, 302 (1966); Lewis v. United States, 385 U.S. 206, 210–11 (1966).
49. Nader v. General Motors, Inc., 225 N.E.2d 765, 770 (N.Y. 1970).
50. See, e.g., Argyll v. Argyll [1967] 1 Ch. 302 (1964) (spouse liable for breach of confidence); Stephens v. Avery, [1988] 1 Ch. 449 (1988) (friend liable for breach of confidence); Barrymore v. News Group Newspapers, [1997] F.S.R. 600 (1997) (lover liable for breach of confidence).
51. Barrymore, *supra,* at 602.
52. *Id.* at 600, 601.
53. Douglas v. *Hello!* Ltd, [2003] 3 All Eng. Rep. 996.
54. Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality,* 96 Geo. L.J. (forthcoming Nov. 2007). The article is available online at http://ssrn.com/abstract=969495.
55. Benjamin Franklin, Poor Richard's Almanac (July 1735) quoted in John Bartlett, Bartlett's Familiar Quotations 309:15 (Justin Kaplan, ed., Little Brown, 16th ed. 1992).
56. Times Mirror Co. v. Superior Court, 244 Cal. Rptr. 556 (Cal. Ct. App. 1988).
57. Y.G. v. Jewish Hospital, 795 S.W.2d 488 (Mo. Ct. App. 1990).
58. Multimedia WMAZ, Inc. v. Kubach, 443 S.E.2d 491 (Ga. 1994).
59. Duran v. Detroit News, Inc., 504 N.W.2d 715 (Mich. Ct. App. 1993).
60. Fisher v. Ohio Department of Rehabilitation and Correction, 578 N.E.2d 901 (Ohio Ct. Cl. 1988).
61. Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy,* 72 U. Chi. L. Rev. 919 (2005).
62. *Id.* at 952, 967.
63. Joanne B. Freeman, *Slander, Poison, Whispers, and Fame: Jefferson's "Anas" and Political Gossip in the Early Republic,* 15 Journal of the Early Republic 25, 33 (1995).
64. *Id.*
65. Giannecchini v. Hospital of St. Raphael, 780 A.2d 1006 (Conn. Super. 2000).
66. Dr. Laura Schlessinger, *Men Leave Because Liberal Feminism Gives Permission,* New Orleans Times Picayune, July 11, 1999, at E7; *Dr. Laura's Anti-Female Rant,* N.Y. Post, Sept. 14, 2006.
67. Patrizia DiLucchio, *Dr. Laura, How Could You?,* Salon.com, Nov. 3, 1998, http://archive.salon.com/21st/feature/1998/11/03feature.html.
68. *Id.*
69. Polly Sprenger, *Dr. Laura Drops Her Suit,* Wired, Dec. 15, 1998, http://wired-vig.wired.com/news/politics/0,1283,16843,00.html.

70. Marcus Errico, *Dr. Laura Dishes on Nude Photos,* E Online, Nov. 4, 1998, http://www.eonline.com/print/index.jsp?uuid=3159acb0-ee3e-454a-ab74-ac7f972390c6&contentType=newsStory.
71. DiLucchio, *Dr. Laura, supra.*
72. 17 U.S.C. §102(a).
73. Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication,* 52 Stan. L. Rev. 1201, 1203 (2002).
74. Lawrence Lessig, *Privacy as Property,* 69 Social Research 247, 250 (2002).
75. Zittrain, *What the Publisher Can Teach the Patient, supra,* at 1206–12.
76. *See, e.g.,* Lawrence Lessig, The Future of Ideas 107–11 (2001); Raymond Shih Ray Ku, *Consumers and Creative Destruction: Fair Use Beyond Market Failure,* 18 Berkeley Tech. L.J. 539, 567 (2003) ("[C]onsumer copying does little to reduce the incentives for creation because, for the most part, the creation of music is not funded by the sale of copies of that music."); Mark A. Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing,* 87 Cal. L. Rev. 113, 124–25 (1999) ("[G]ranting property rights to original creators allows them to prevent subsequent creators from building on their works, which means that a law designed to encourage the creation of first-generation works may actually risk stifling second-generation creative works."); Neil Weinstock Netanel, *Copyright and a Democratic Civil Society,* 106 Yale L.J. 283, 295 (1996) ("An overly expanded copyright also constitutes a material disincentive to the production and dissemination of creative, transformative uses of preexisting expression.").
77. Eldred v. Ashcroft, 537 U.S. 186, 190 (2003) (declaring that copyright is "compatible with free speech principles.").
78. Restatement (Second) of Torts §652C.
79. Jonathan Kahn, *Bringing Dignity Back to Light: Publicity Rights and the Eclipse of the Tort of Appropriation of Identity,* 17 Cardozo Arts & Ent. L.J. 213, 223 (1999).
80. Pavesich v. New England Life Insurance Co., 50 S.E. 68, 70 (Ga. 1905).
81. *Id.* at 80.
82. William Prosser, *Privacy,* 48 Cal. L. Rev. 383, 406 (1960).
83. Paulsen v. Personality Posters, Inc., 299 NYS2d 501 (1968).
84. Rosemont Enterprises, Inc. v. Random House, Inc., 294 N.Y.S.2d 122 (1968).
85. *See* Hosking v. Runting, [2004] NZCA 34, at [46] ("As the law currently stands, a successful action requires information that is confidential, communication of that information to another in circumstances importing an obligation of confidence and unauthorised use or disclosure."); International Corona v. Lac Minerals, [1989] 2 S.C.R. 574 (stating elements of breach-of-confidentiality tort); ABC v. Lenah, [2004] HCA 63, at [34] (discussing the breach-of-confidentiality tort).