INTERNET LAW: CASES AND PROBLEMS

James Grimmelmann
Associate Professor of Law
New York Law School

www. semaphorepress.com

For my parents.

Internet Law: Cases and Problems

James Grimmelmann

INTERNET LAW: CASES AND PROBLEMS

James Grimmelmann

TABLE OF CONTENTS **BOOK PAGE #**

INTRODUCTION

Welcome to Internet Law.

Innocuous as that sentence may sound, it conceals two controversial assumptions. The first is whether something like "Internet law" even exists as its own subject; the second is whether "Internet law" is the right name for it.

Does Internet Law Exist?

If you flip through the table of contents of this book, you will see topics drawn from all across the law, including jurisdiction, free speech, privacy, tort, contract, criminal procedure and criminal law, trademark, copyright, antitrust, and telecommunications law. This diversity is characteristic of the field. It also requires us to ask whether this is a field worth studying.

In 1996, Judge Frank Easterbrook was asked to speak to a conference at the University of Chicago Law School on "The Law of Cyberspace." His remarks, which bore the title "Cyberspace and the Law of the Horse," have become famous for throwing down a gauntlet at the feet of the assembled scholars. He questioned whether it made sense to talk about "cyberspace law" or "computer law" or "Internet law" at all.

> When he was dean of this law school, Gerhard Casper was proud that the University of Chicago did not offer a course in "The Law of the Horse." He did not mean by this that Illinois specializes in grain rather than livestock. His point, rather, was that "Law and . . ." courses should be limited to subjects that could illuminate the entire law. …
>
> Dean Casper's remark had a second meaning – that the best way to learn the law applicable to specialized endeavors is to study general rules. Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on "The Law of the Horse" is doomed to be shallow and to miss unifying principles. Teaching 100 percent of the cases on people kicked by horses will not convey the law of torts very well. Far better for most students – better, even, for those who plan to go into the horse trade – to take courses in property, torts, commercial transactions, and the like, adding to the diet of horse cases a smattering of transactions in cucumbers, cats, coal, and cribs. Only by putting the law of the horse in the context of broader rules about commercial endeavors could one really understand the law about horses.
>
> Now you can see the meaning of my title. When asked to talk about "Property in Cyberspace," my immediate reaction was, "Isn't this just the law of the horse?" [*]

To this day, "the law of the horse" is a code phrase among Internet-law scholars for the idea that there's nothing new here, that studying Internet law is nothing more than an exercise in applying unrelated bodies of law to the Internet, with no unifying doctrines or truly distinctive insights. Almost since Easterbrook sat down at the end of his talk, scholars have been debating whether he was right. During your study of Internet law, you should be asking yourself whether the subject really does "illuminate the entire law"

---

[*] Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 207–08 (1996).

As a starting point, here are some possible responses to the question.

- *Easterbrook Was Right*. Internet law is necessarily a patchwork. Maybe the effort spent learning a little antitrust law and a little privacy law and a little First Amendment law would be better spent learning one of them in depth. Perhaps this course is best understood as a sampler platter: a bit of each so you can have a better sense of what else there is to know about.
- *Internet Issues Overlap*. The same simple few facts may raise copyright, contract, and criminal issues. The way you analyze one will affect how you analyze the others. Or, a problem may require a difficult characterization: should we think of this as a free-speech matter, a telecommunications question, or an antitrust issue? Again, you will need to draw on multiple bodies of law and put them into conversation with each other.
- *The Internet Is Too Important to Ignore*. As a lawyer, you will need to handle the problems your clients bring to you. Increasingly often, those problems involve the Internet. Family law changes when children's Facebook pages become admissible evidence; securities law changes when people do worldwide fundraising from a webpage. To counsel your clients effectively, you need to have a clear picture of how the Internet works and what people are doing with it.
- *Some Law Is Internet-Only*. When Easterbrook spoke in 1996, Internet law was largely a blank slate. Today, that is no longer true. Major pieces of legislation, such as the 1996 Communications Decency Act and the 1998 Digital Millennium Copyright Act, have created important bodies of Internet-specific law. Some of these doctrines are likely to surprise you – they've certainly surprised lawyers who didn't expect that law online might not be the same as law offline.
- *There Are Patterns in Internet Law*. Even when doing Internet law just consists in applying familiar doctrines to online activities, some problems crop up again and again. It can be harder to tell precisely where a tort took place, for example, when the plaintiff, the defendant, and the computers they used to communicate are all in different countries. This is a problem for copyright, for defamation, for taxation... and so on. By studying how different bodies of law have been applied to online activity, you can gain a feel for how other bodies of law might apply to Internet facts.
- *Maybe the Internet Does Change Everything*. Easterbrook's analogy assumes a world in which most torts and transactions don't involve horses. Nor did horses radically transform American society. But the Internet is changing how we live, think, write, love, fight, do business, and think of ourselves. Some of those changes may go so deep that they call into question basic assumptions on which areas of law are based. Studying the ways in which our legal system has tried to grapple with those changes may give you a handle on what else may be coming.

These are only possibilities. Perhaps you will agree with one or more. Perhaps you will reject them all.

"Internet" and "Cyberspace"

Judge Easterbrook didn't mention "Internet law" in his presentation. Instead, he discussed the "law of cyberspace." That term carries a lot of baggage, and there's a reason this book mostly doesn't use it.

"Cyberspace" was coined by the science fiction novelist William Gibson to describe a new *place* created by worldwide computer networks. Here is a description of it from his 1984 novel *Neuromancer*:

> On the Sony, a two-dimensional space war faded behind a forest of mathematically generated ferns, demonstrating the spacial possibilities of logarithmic spirals; cold blue military footage burned through, lab animals

> wired into test systems, helmets feeding into fire control circuits of tanks and war plans. 'Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts . . . A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity, Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding. . . .*

The idea that networked computers would create a wholly new place with its own geography, imagery, and laws of physics was nearly irresistible for science-fiction novelist and Hollywood filmmakers. While some movies, like *WarGames* (1983) were "realistic" in the sense that they showed computer users typing commands and looking at the results on their screens, others imagined that the future of computing would involve highly immersive virtual realities. *The Matrix* (1999) took this idea about as far as it could go.

Meanwhile, it was apparent to many lawyers and scholars that computers were posing interesting legal issues, such as the proper telecommunications regulation of computer networks, the copyrightability of computer software, and liability for programming defective computer systems. Looking ahead, many also expected that computer networks (and eventually and especially the Internet) were going to raise questions about some seemingly fundamental legal concepts.

For example, consider jurisdiction. If two people across the globe from each other could interact instantaneously and profoundly with each other, perhaps it made more sense to say that their interaction happened "in cyberspace" rather than in the country either one of them was in. And if so, then wouldn't it follow the most appropriate body of law to apply would be a new body of "cyberspace law" that took the mind-bending possibilities of computers seriously, that was specially adapted for the new physics and new customs of cyberspace?

Thinking of new laws in terms of "cyberspace," however, emphasizes a particular vision of the form those laws would take. It suggests that cyberspace is somewhere separate and apart from the rest of the world, that when you go online you really are *going* somewhere and leaving your offline home behind. It suggests a kind of simple territoriality for law: cyberlaw applies in cyberspace, just as Swedish law applies in Sweden. And it creates a sharp division between offline and online conduct and laws.

With the benefit of hindsight, though, it hasn't turned out that way. As the Internet has grown in importance, it has increasingly permeated daily life. Rather than being a place people go to leave their regular lives behind, the Internet is something they welcome into their lives in innumerable ways. In addition, the science-fiction novelists got at least one thing very wrong. For most people, there is no one "cyberspace." Instead, there are all sorts of things online, and the way we experience them varies enormously. Shopping for shoes on eBay is a different experience from having a video chat on Skype, and the legal regimes involved take account of those differences.

This casebook, therefore, deals with "Internet law" rather than "cyberspace law" or "cyberlaw." Judges, lawyers, and clients use the Internet, not cyberspace, and the book reflects that reality. At the same time, it is important to think about the role that the idea of cyberspace has played in shaping Internet law. Some doctrines still bear its traces. There are also important debates about how strongly Internet law should resemble offline law, and in the course of this book, we will engage with many of them.

---

* WILLIAM GIBSON, NEUROMANCER 51 (Penguin 2000).

About the Book

This book is arranged around four major themes in Internet law:

- *Code is Law*: how does regulation change when it's carried out by computers, rather than by people*?*
- *Governmental Control*: Does going online increase or decrease government control?
- *Intermediary Power*: What kinds of power do online intermediaries possess?
- *Generativity*: What are the causes and consequences of the extraordinary level of innovation and creativity on the Internet?

Each chapter raises questions about two or more of these themes. Keep alert for them as you read; they will help you connect the dots between different doctrines.

This is not a "hide the ball" casebook. The subject is hard enough without introducing artificial difficulties. The notes and questions following each case are meant to help you think through the legal questions faced by the court, the implications of its holding for future cases, and the policy issues lurking in the background. You do not need to have the correct answer (indeed, many questions have no single "correct" answer), but it is important to consider them all.

Some sections of this book contain statutory excerpts. The questions following them are especially important. Statute-reading is a critical skill for a lawyer, but it is hard work and it takes practice. The questions are intended to give you a guided walkthrough of the process, helping you develop your mental agility as you flip between definitions, applications, and exceptions.

You may also have noticed that most sections contain one or more problems. They are an integral part of this casebook, and they are designed to be hard but doable. Some of them introduce doctrinal or factual twists not covered in the cases and notes. Others require you to exercise negotiation, counseling, and strategic skills. They are all drawn from real problems faced by real lawyers, and if they were able to find good solutions for their clients, you can too. Do not be afraid to draw on what you have learned in other courses, or in your life outside of law school.

Finally, despite all these dire warnings, this casebook is meant to be fun. It is almost impossible to flip through a newspaper or browse a website without coming across an Internet law issue. By the time you finish with this book, you will be able to spot these issues, put them in context, and impress your friends with your real-life knowledge. I have tried to select cases with vivid, memorable facts; Internet law in general has no shortage of them. I have enjoyed every minute of teaching the subject and preparing this casebook; I hope that you will enjoy your time with it, too.

Notes on the Editing

I have indicated the omission of textual material with an ellipsis ("…"), to distinguish them from omissions in the source (". . ."). An ellipsis may indicate the omission of anywhere from a few words to multiple pages, except in statutory excerpts, where I have used an ellipsis at each level of omitted structure. I have omitted footnotes and citations without indication, and sometimes moved or replaced them for clarity. I have also sometimes removed quotation marks from within an edited opinion, along with the citation to the source being quoted. Footnotes in cases are numbered as in the original. I have for the most part standardized judge's names as "Lastname, Title" – except for the Supreme Court's traditional formula: "Justice Lastname delivered the opinion of the Court."

Acknowledgments

In addition to designing a fairer casebook business model, my editors at Semaphore Press, Lydia Pallas Loren and Joseph Scott Miller, did me the great favor of holding this book to their own high standards. Robert Heverly at Albany Law School taught from a draft of what became this casebook and gave me numerous useful suggestions. My colleagues Richard Chused, Dan Hunter, David Johnson, Beth Noveck, and Molly Land will recognize many of their ideas in these pages. Aislinn Black, who knows more Internet law than many lawyers, was generous with her wisdom.

I am grateful to the students in my Internet Law courses at New York Law School, on whom I tested earlier versions of this book. Their judgments about what worked and what didn't made this book what it is. The book would also not have been possible without the hard work of my research assistants over the years: Catherine Baxter, Cynthia Grady, James Major, Dominic Mauro, and Joseph Merante. Their diligence and imagination helped turn a sprawling packet of cases into a focused casebook. A very special thanks to Linda Torosian.

Permissions

CHAPTER 1: COMPUTERS

The first of the four major themes of this book is how law changes when computers – rather than people – make and enforce decisions. It is arguably *the* central question in all of Internet law. Although he was not the first to focus on the question, Professor Lawrence Lessig gave the most influential answer to it: "code is law." By this, he meant that computer software (or "code") could do some of the same work that law ordinarily does in controlling people's conduct. This chapter explores the idea with two case studies of regulation by software: responsibility for computer errors, and computer evidence.

I. Theory

LAWRENCE LESSIG, CODE 2.0
121–26 (2006)

A Dot's Life

There are many ways to think about "regulation." I want to think about it from the perspective of someone who is regulated, or, what is different, constrained. That someone regulated is represented by this (pathetic) dot – a creature (you or me) subject to different regulations that might have the effect of constraining (or as we'll see, enabling) the dot's behavior. By describing the various constraints that might bear on this individual, I hope to show you something about how these constraints function together.

Here then is the dot.

How is this dot "regulated"

Let's start with something easy: smoking. If you want to smoke, what constraints do you face? What factors regulate your decision to smoke or not?

One constraint is legal. In some places at least, laws regulate smoking – if you are under eighteen, the law says that cigarettes cannot be sold to you. If you are under twenty-six, cigarettes cannot be sold to you unless the seller checks your ID. Laws also regulate where smoking is permitted – not in O'Hare Airport, on an airplane, or in an elevator, for instance. In these two ways at least, laws aim to direct smoking behavior. They operate as a kind of constraint on an individual who wants to smoke.

But laws are not the most significant constraints on smoking. Smokers in the United States certainly feel their freedom regulated, even if only rarely by the law. There are no smoking police, and smoking courts are still quite rare. Rather, smokers in America are regulated by norms. Norms say that one doesn't light a cigarette in a private car without first asking permission of the other passengers. They also say, however, that one needn't ask permission to smoke at a picnic. Norms say that others can ask you to stop smoking at a restaurant, or that you never smoke during a meal. These norms effect a certain constraint, and this constraint regulates smoking behavior.

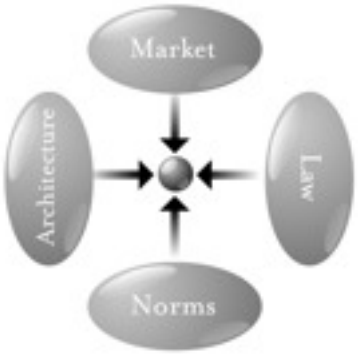
Laws and norms are still not the only forces regulating smoking behavior. The market is also a constraint. The price of cigarettes is a constraint on your ability to smoke – change the price, and you change this constraint. Likewise with quality. If the market

supplies a variety of cigarettes of widely varying quality and price, your ability to select the kind of cigarette you want increases; increasing choice here reduces constraint.

Finally, there are the constraints created by the technology of cigarettes, or by the technologies affecting their supply. Nicotine-treated cigarettes are addictive and therefore create a greater constraint on smoking than untreated cigarettes. Smokeless cigarettes present less of a constraint because they can be smoked in more places. Cigarettes with a strong odor present more of a constraint because they can be smoked in fewer places. How the cigarette is, how it is designed, how it is built – in a word, its architecture – affects the constraints faced by a smoker.

Thus, four constraints regulate this pathetic dot – the law, social norms, the market, and architecture – and the "regulation" of this dot is the sum of these four constraints. Changes in any one will affect the regulation of the whole. Some constraints will support others; some may undermine others. Thus, "changes in technology [may] usher in changes in . . . norms," [8] and the other way around. A complete view, therefore, must consider these four modalities together.

So think of the four together like this:



In this drawing, each oval represents one kind of constraint operating on our pathetic dot in the center. Each constraint imposes a different kind of cost on the dot for engaging in the relevant behavior – in this case, smoking. The cost from norms is different from the market cost, which is different from the cost from law and the cost from the (cancerous) architecture of cigarettes.

The constraints are distinct, yet they are plainly interdependent. Each can support or oppose the others. Technologies can undermine norms and laws; they can also support them. Some constraints make others possible; others make some impossible. Constraints work together, though they function differently and the effect of each is distinct. Norms constrain through the stigma that a community imposes; markets constrain through the price that they exact; architectures constrain through the physical burdens they impose; and law constrains through the punishment it threatens.

We can call each constraint a "regulator," and we can think of each as a distinct modality of regulation. Each modality has a complex nature, and the interaction among these four is also hard to describe. [F]or now, it is enough to see that they are linked and that, in a sense, they combine to produce the regulation to which our pathetic dot is subject in any given area.

We can use the same model to describe the regulation of behavior in cyberspace.

Law regulates behavior in cyberspace. Copyright law, defamation law, and obscenity laws all continue to threaten ex post sanction for the violation of legal rights.

---

[8] [J.D. Lasica], *Darknet* 16 [(2005)].

How well law regulates, or how efficiently, is a different question: In some cases it does so more efficiently, in some cases less. But whether better or not, law continues to threaten a certain consequence if it is defied. Legislatures enact; prosecutors threaten; courts convict.

Norms also regulate behavior in cyberspace. Talk about Democratic politics in the alt.knitting newsgroup, and you open yourself to flaming; "spoof" someone's identity in a MUD [Multi-User Dungeon, a kind of early, text-based virtual world[, and you may find yourself "toaded"; talk too much in a discussion list, and you are likely to be placed on a common bozo filter. In each case, a set of understandings constrain behavior, again through the threat of ex post sanctions imposed by a community.

Markets regulate behavior in cyberspace. Pricing structures constrain access, and if they do not, busy signals do. (AOL learned this quite dramatically when it shifted from an hourly to a flat-rate pricing plan.) Areas of the Web are beginning to charge for access, as online services have for some time. Advertisers reward popular sites; online services drop low-population forums. These behaviors are all a function of market constraints and market opportunity. They are all, in this sense, regulations of the market.

Finally, an analog for architecture regulates behavior in cyberspace – code. The software and hardware that make cyberspace what it is constitute a set of constraints on how you can behave. The substance of these constraints may vary, but they are experienced as conditions on your access to cyberspace. In some places (online services such as AOL, for instance) you must enter a password before you gain access; in other places you can enter whether identified or not. In some places the transactions you engage in produce traces that link the transactions (the "mouse droppings") back to you; in other places this link is achieved only if you want it to be.

In some places you can choose to speak a language that only the recipient can hear (through encryption); in other places encryption is not an option. The code or software or architecture or protocols set these features, which are selected by code writers. They constrain some behavior by making other behavior possible or impossible. The code embeds certain values or makes certain values impossible. In this sense, it too is regulation, just as the architectures of real-space codes are regulations. ...

On Governments and Ways to Regulate

I've described four constraints that I've said "regulate" an individual. But these separate constraints obviously don't simply exist as givens in a social life. They are neither found in nature nor fixed by God. Each can be changed, though the mechanics of changing them is complex. Law can have a significant role in this mechanics, and my aim in this section is to describe that role.

A simple example will suggest the more general point. Say the theft of car radios is a problem – not big in the scale of things, but a frequent and costly enough problem to make more regulation necessary. One response might be to increase the penalty for car radio theft to life in prison, so that the risk faced by thieves made it such that this crime did not pay. If radio thieves realized that they exposed themselves to a lifetime in prison each time they stole a radio, it might no longer make sense to them to steal radios. The constraint constituted by the threatened punishment of law would now be enough to stop the behavior we are trying to stop.

But changing the law is not the only possible technique. A second might be to change the radio's architecture. Imagine that radio manufacturers program radios to work only with a single car – a security code that electronically locks the radio to the car, so that, if the radio is removed, it will no longer work. This is a code constraint on the theft of radios; it makes the radio no longer effective once stolen. It too functions as a constraint on the radio's theft, and like the threatened punishment of life in prison, it could be effective in stopping the radio-stealing behavior.

Thus, the same constraint can be achieved through different means, and the different means cost different amounts. The threatened punishment of life in prison may be fiscally more costly than the change in the architecture of radios (depending on how many people actually continue to steal radios and how many are caught). From this fiscal perspective, it may be more efficient to change code than law. Fiscal efficiency may also align with the expressive content of law – a punishment so extreme would be barbaric for a crime so slight. Thus, the values may well track the efficient response. Code would be the best means to regulate.

The costs, however, need not align so well. Take the Supreme Court's hypothetical example of life in prison for a parking ticket. It is likely that whatever code constraint might match this law constraint, the law constraint would be more efficient (if reducing parking violations were the only aim). There would be very few victims of this law before people conformed their behavior appropriately. But the "efficient result" would conflict with other values. If it is barbaric to incarcerate for life for the theft of a radio, it is all the more barbaric as a penalty for a parking violation. The regulator has a range of means to effect the desired constraint, but the values that these means entail need not align with their efficiency. The efficient answer may well be unjust – that is, it may conflict with values inherent in the norms, or law (constitution), of the society

Questions

1. Lessig's "four modalities" are famous among Internet scholars. What are they? Consider a familiar problem: littering. How can law deal with littering? What can markets do to reduce littering? How do social norms affect whether people litter or not? And can you think of any architectural factors that encourage or discourage littering?

2. Lessig also calls attention to the interactions among modalities. How can software substitute for law? How can software make law more effective? How can software undermine legal control? Try to give an example of each.

3. Although he famously summed up his theory with the phrase "code is law," part of Lessig's point is precisely that software *isn't the same* as law. Instead, he describes computer software as a kind of "architecture." Why does he use that word? How accurate is the metaphor?

II. Computers and Errors

The cases in this section involve people who have interacted with a computer that has apparently made a mistake. The question facing each court is how to apply traditional legal standards once a computer enters the picture. Don't worry about trying to learn the substantive doctrines of banking law or public utilities law. Instead, determine what the rule would be if there weren't a computer involved, and then ask whether that rule makes sense in a "computerized" context. As we'll see – repeatedly – even when there's no doubt that law applies "to computers," figuring out *how* law applies in a new factual context can be a tricky problem.

Question

1. Have you ever dealt with a customer service agent who couldn't help you because "the computer" wouldn't allow it? Have you ever been unable to buy something because the sales clerk couldn't get "the computer" to work? Why are computers so often associated with bureaucracy and frustration?

Kennison v. Daire
High Court of Australia
[1986] HCA 4

Gibbs, Chief Justice:

The appellant was convicted of larceny. ... He was the holder of an Easybank card which enabled him to use the automatic teller machine of the Savings Bank of South Australia to withdraw money from his account with that bank. It was a condition of the use of the card that the customer's account could be drawn against to the extent of the funds available in that account. Before the date of the alleged offence, the appellant had closed his account and withdrawn the balance, but had not returned the card. On the occasion of the alleged offence, he used his card to withdraw $200 from the machine at the Adelaide branch of the bank. He was able to do so because the machine was off-line and was programmed to allow the withdrawal of up to $200 by any person who placed the card in the machine and gave the corresponding personal identification number. When off-line the machine was incapable of determining whether the card holder had any account which remained current, and if so, whether the account was in credit.

It is not in doubt that the appellant acted fraudulently with intent permanently to deprive the bank of $200. The appellant's submission is that the bank consented to the taking. It is submitted that the bank intended that the machine should operate within the terms of its programme, and that when it did so it gave effect to the intention of the bank.

In the course of an interesting argument, Mr Tilmouth pointed out that if a teller, having the general authority of the bank, pays out money on a cheque when the drawer's account is overdrawn, or on a forged order, the correct conclusion is that the bank intends that the property in the money should pass, and that the case is not one of larceny. ... He submitted that, in effect, the machine was invested with a similar authority and that if, within the instructions in its programme, it handed over the money, it should be held that the property in the money passed to the card holder with the consent of the bank.

With all respect we find it impossible to accept these arguments. The fact that the bank programmed the machine in a way that facilitated the commission of a fraud by a person holding a card did not mean that the bank consented to the withdrawal of money by a person who had no account with the bank. It is not suggested that any person, having the authority of the bank to consent to the particular transaction, did so. The machine could not give the bank's consent in fact and there is no principle of law that requires it to be treated as though it were a person with authority to decide and consent.

The proper inference to be drawn from the facts is that the bank consented to the withdrawal of up to $200 by a card holder who presented his card and supplied his personal identification number, only if the card holder had an account which was current. It would be quite unreal to infer that the bank consented to the withdrawal by a card holder whose account had been closed. The conditions of use of the card supplied by the bank to its customers support the conclusion that no such inference can be drawn. It is unnecessary to consider what the position might have been if the account had remained current but had insufficient funds to its credit. ...

For these reasons ... the appeal should be dismissed.

Pompeii Estates, Inc. v. Consolidated Edison Co. of N.Y., Inc.

397 N.Y.S.2d 577 (Civ. Ct. N.Y.C. 1977)

Posner, J.:

The "Dawn of the Age of Aquarius" has also ushered in the "Age of the Computer."

There is no question that the modern computer is as indispensable to big business as the washing machine is to the American household. To ask the American housewife to go back to washing clothes by hand is as unthinkable as asking Consolidated Edison to send out its monthly bills by any other method than the computer.

This is an action in negligence by a builder against a public utility for damages sustained as a result of the alleged "wrongful" termination of electricity at an unoccupied one-family house (that had recently been constructed by the plaintiff) at 200-15 Pompeii Rd., Holliswood. Sometime in October, 1975, the defendant had installed electric services to the plaintiff's property. On or about January 20, 1976, the defendant terminated such service because of two unpaid bills amounting to $25.11. Since the premises were unoccupied, the lack of electricity caused the motor which operated the heating unit to go off, which resulted in frozen water pipes, which burst and caused $1,030 of proven damages to the premises. ...

Defendant through the use of five witnesses, made out a good case proving that the notice to disconnect was probably mailed even though no witness had actual knowledge of mailing this specific notice. Obviously, it would be overly burdensome, if not impossible, to expect a utility mailing out thousands of disconnect notices a day to be able to prove that each one was individually mailed. ...

Accordingly, this court finds that the defendant did comply with the statutory requirement of mailing even though we are also convinced that the plaintiff had never received the notice because an expert witness from the U.S. Postal Department testified that the postal service does not leave mail at an unoccupied address. Unless a statute or the contract between the parties calls for actual notice proof of mailing is sufficient to prove notice, even though the notice was never received.

While the parties, at the trial and in their memoranda of law devoted considerable time to the issue of "notice", the court finds that this is not the main issue in this case. Let us say that this was a "procedural" hurdle which Consolidated Edison cleared successfully. However, the court has serious doubts as to whether the defendant has cleared the "substantive" hurdle – did it act reasonably or negligently in discontinuing plaintiff's electric service?

... The defendant's witnesses stated that a customer's file is opened when a new account is established and that all correspondence and other documents involving the customer are included in this file. Defendant's attorney admitted that he had found in such file the original letter from plaintiff requesting the opening of electrical current. This letter is reproduced in its entirety because of its significance to the case:

POMPEII ESTATES INC.
34-34 Bell Blvd.
Bayside, N.Y. 11361
212-631-4466

June 12, 1975

Con Edison
40-55 College Pt. Blvd.
Flushing, N.Y. 11354
Att: Mr. A. Vebeliunas – 670-6152

To Whom It May Concern:

Please be advised that there have been no changes in the original Building Plans for the 2 Houses located at the following addresses:

House #1-200-15 Pompeii Rd., Holliswood, N.Y. – Lot #163
House #2 – 200-19 Pompeii Rd., Holliswood, N.Y. – Lot #160

Be further advised that the electrical load within the house will be:

6KW Lighting and 3 1/2 Horse Power Air-Conditioning
1/4 Horse Power Blowers
1.2 KW Dishwashers

There will be 1-150 AMP – 3 wire socket type electric meter for each house.

Sincerely yours,

POMPEII ESTATES
AT: SWR
ALBINO TESTANI – PRESIDENT

Between the date of this letter (June 12, 1975) and the time service was installed (Oct. 24, 1975) four months elapsed. There was no other correspondence; but the plaintiff's witness (Testani) testified that he had numerous conversations with Mr. Vebeliunas on the phone and at the job site. Mr. Vebeliunas, defendant's employee never appeared in court, even though the case was tried on three separate occasions over a period of two weeks. Though Vebeliunas was defendant's field representative and the only contact plaintiff had with defendant, he was never consulted when the decision was made to discontinue service for the nonpayment of the first two months rent. The testimony of defendant's witnesses bore out the fact that said decision was a routine procedure activated by the computer and ordered by a Mr. Chris Hagan. Did defendant produce Mr. Hagan to testify what human input there was to the computer's order? No, like Mr. Vebeliunas, he never graced the courtroom scene. Failure to produce two key witnesses under the defendant's control can only lead to the inference that they would not contradict the plaintiff's contention that defendant acted unreasonably.

Negligence is lack of ordinary care. It is a failure to exercise that degree of care which a reasonably prudent person would have exercised under such circumstances. The statute only requires the notice of discontinuance to be sent to the premises where the service is provided; though, by regulation, the Public Service Commission has said that the customer may direct another address for mailing purposes. While the plaintiff's letter (*supra*) does not specifically direct that the mail be sent to 34-34 Bell Boulevard, any reasonably prudent person examining the letter would realize that this is a builder building new homes and that it is not customary for a builder to occupy the homes he builds. Certainly, any reasonably prudent person, if in doubt, would contact Mr. Vebeliunas to ascertain the facts. This is especially so when the termination of service is in the middle of winter and the foreseeable consequences to the heating system and the

water pipes are apparent. Where there is a foreseeability of damage to another that may occur from one's acts, there arises a duty to use care. In this instance, a one-minute cursory glance at plaintiff's letter (*supra*) would have alerted Mr. Hagan to the fact that there was something unusual in this situation. To the contrary, the computer said, "terminate," and Mr. Hagan gave the order to terminate.

This court finds the defendant liable to the plaintiff for damages in the amount of $1,030, with interest and costs. While the computer is a useful instrument, it cannot serve as a shield to relieve Consolidated Edison of its obligation to exercise reasonable care when terminating service. The statute gives it the discretionary power to do so, and this discretion must be exercised by a human brain. Computers can only issue mandatory instructions – they are not programmed to exercise discretion.

Questions

1. *Kennison* implies that the result would have been different if the defendant had dealt with a human, rather than with a computer. Why? Would the result in *Pompeii Estates* have been different if the defendants there had dealt with a human, rather than a computer?

2. Does the law treat computers as people? Should it?

3.Who programmed the computer in *Kennison*? Who programmed the computer in *Pompeii Estates*? Did any of them make mistakes in what they programmed the computers to do?

4.Why did Easybank use a computer? Why did ConEd? What advantages does a computer provide? What are the disadvantages? Would society be better off if we prohibited the use of computers for these purposes altogether? If not, what safeguards do we need on their use?

5.If you receive some information from a computer, are you allowed to take the computer at its word? If you put information into a computer, are you now responsible for all the consequences? What about the person who provides the computer? The person who programmed it? Who, if anyone, *ought* to be held responsible?

NCIC Confidential Problem

You represent Archibald Buttle, a resident of Carrollton, Michigan, who has repeatedly been arrested for crimes he didn't commit. In October 2009, Buttle saw a neighbor preparing to cut a tree from his, Buttle's, land. The two of them got into a heated argument, with the neighbor claiming that the tree was a danger in case of a storm. Someone called the police, and Patrolman Jack Vincennes of the Carrollton Township Police Department responded to the call. Patrolman Vincennes broke up the fight, then put Buttle's name into the National Crime Information Center (NCIC) computer network run by the FBI. The NCIC network reported that there was an outstanding warrant for his arrest in California on charges of robbery and murder.

Buttle spent four days in jail while the Carrollton police contacted the Los Angeles Police Department (LAPD) about the warrant. Sergeant Ed Exley of the LAPD reported that an "Archibald Buttle" had been arrested in Los Angeles in July 2008 on suspicion of murder. He had been released several days later, but additional evidence discovered in early August 2008 had convinced the LAPD that Buttle was their man. By that time, however, he had disappeared, and so Lieutenant Dudley Smith of the LAPD had a warrant issued for Buttle's arrest and entered the warrant into the NCIC's computer network.

On being informed of this, your client loudly protested that there must have been a mistake, that he hadn't been to California in over a decade. On the fourth day of his confinement, a comparison of his fingerprints and physical description with the LAPD's files definitively showed that your client was not the man wanted in California, who had

several distinctive scars and tattoos. Buttle was released. Further investigation by Patrolman Vincennes revealed that one Rollo Tomasi, an escapee from an Alabama prison, had obtained a copy of your client's birth certificate and used it to obtain a California driver's license in the name of "Archibald Buttle."

When your client was arrested, the entry for the warrant was automatically purged from the NCIC system. In November 2009, Lieutenant Smith reentered the arrest warrant in Buttle's name in the NCIC system. Each entry in the NCIC system has, in addition to name, charges, warrant number, and issuing jurisdiction, a "miscellaneous" field that allows for the entry of up to 121 characters. Lieutenant Smith did not enter any information in that field.

In March 2010, Buttle was driving when he was stopped by Bay County sheriff's deputy Bud White outside of Saginaw, Michigan, for failure to use a turn signal. Deputy White took Buttle's driver's license and checked the name against the NCIC system, turning up the California warrant. As a result, Deputy White ordered Buttle out of the car at gunpoint, then searched, handcuffed, and arrested him. He was released after about two hours, when Deputy White had made phone calls to the Saginaw Police and the LAPD.

Buttle has been arrested three more times, twice at gunpoint, by police in Michigan and Texas. Each time, he was released after his true identity was confirmed. He sought the assistance of the FBI, who confirmed that the NCIC contained a murder warrant in his name, but informed Buttle that "only the originating state agency (i.e. the LAPD) could delete, amend, or correct the computer warrant entry."

Buttle has come to you for legal advice. He would like to stop being arrested for crimes he didn't commit and, if possible, recover damages for the past arrests. What, if anything, can he do?

III. Computer Evidence

As a further example of the ways in which computers raise distinctive issues even outside of "computer cases," consider the field of evidence law. Every case depends on evidence, which is to say that evidentiary problems pervade the entire law. The legal system has worked out rules and doctrines that govern both the substantive law of evidence (what evidence does or does not "count" toward a factual conclusion) and the procedures by which it is introduced and assessed (e.g the familiar sequence of direct and cross examination). This section considers a few of the special issues that can arise when some of that evidence is stored on computers. Both of the cases involve social networking sites, but the issues are more general.

Griffin v. State

419 Md. 343 (2011)

Battaglia, Judge:

In this case, we are tasked with determining the appropriate way to authenticate, for evidential purposes, electronically stored information printed from a social networking website, in particular, MySpace.[2]

Antoine Levar Griffin, Petitioner, seeks reversal of his convictions in the Circuit Court for Cecil County, contending that the trial judge abused his discretion in admitting, without proper authentication, what the State alleged were several pages printed from Griffin's girlfriend's MySpace profile. ...

Griffin was charged in numerous counts with the shooting death, on April 24, 2005, of Darvell Guest at Ferrari's Bar in Perryville, in Cecil County. During his trial, the State sought to introduce Griffin's girlfriend's, Jessica Barber's, MySpace profile to demonstrate that, prior to trial, Ms. Barber had allegedly threatened another witness called by the State. The printed pages contained a MySpace profile in the name of "Sistasouljah," describing a 23 year-old female from Port Deposit, listing her birthday as "10/02/1983" and containing a photograph of an embracing couple. The printed pages also contained the following blurb:

> FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!

When Ms. Barber had taken the stand after being called by the State, she was not questioned about the pages allegedly printed from her MySpace profile.

Instead, the State attempted to authenticate the pages, as belonging to Ms. Barber, through the testimony of Sergeant John Cook, the lead investigator in the case. Defense counsel objected to the admission of the pages allegedly printed from Ms. Barber's MySpace profile, because the State could not sufficiently establish a "connection" between the profile and posting and Ms. Barber ...

Whether the MySpace printout represents that which it purports to be, not only a MySpace profile created by Ms. Barber, but also upon which she had posted, "FREE

---

[2] "MySpace is a 'social networking' website where members can create 'profiles' and interact with other members. Anyone with Internet access can go onto the MySpace website and view content which is open to the general public such as a music area, video section, and members' profiles which are not set as 'private.' However, to create a profile, upload and display photographs, communicate with persons on the site, write 'blogs,' and/or utilize other services or applications on the MySpace website, one must be a 'member.' Anyone can become a member of MySpace at no charge so long as they meet a minimum age requirement and register." *United States v. Drew*, 259 F.R.D. 449, 453 (D.Cal.2009).

BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!," is the issue before us.

Anyone can create a MySpace profile at no cost, as long as that person has an email address and claims to be over the age of fourteen ...

The identity of who generated the profile may be confounding ... because anyone can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password ...

The potential for fabricating or tampering with electronically stored information on a social networking site, thus poses significant challenges from the standpoint of authentication of printouts of the site, as in the present case. Authentication, nevertheless, is generally governed by Maryland Rule 5–901, which provides:

> (a) General provision. The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

Potential methods of authentication are illustrated in Rule 5–901(b). The most germane to the present inquiry are Rules 5–901(b)(1) and 5–901(b)(4), which state:

> (b) Illustrations. By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this Rule:
>
> > (1) Testimony of witness with knowledge. Testimony of a witness with knowledge that the offered evidence is what it is claimed to be.
> >
> > * * *
> >
> > (4) Circumstantial evidence. Circumstantial evidence, such as appearance, contents, substance, internal patterns, location, or other distinctive characteristics, that the offered evidence is what it is claimed to be.

... In the present case, Griffin argues that the State did not appropriately, for evidentiary purposes, authenticate the pages allegedly printed from Jessica Barber's MySpace profile, because the State failed to offer any extrinsic evidence describing MySpace, as well as indicating how Sergeant Cook obtained the pages in question and adequately linking both the profile and the "snitches get stitches" posting to Ms. Barber. The State counters that the photograph, personal information, and references to freeing "Boozy" were sufficient to enable the finder of fact to believe that the pages printed fromMySpace were indeed Ms. Barber's. ...

We agree with Griffin that the trial judge abused his discretion in admitting the MySpace evidence pursuant to Rule 5–901(b)(4), because the picture of Ms. Barber, coupled with her birth date and location, were not sufficient "distinctive characteristics" on a MySpace profile to authenticate its printout, given the prospect that someone other than Ms. Barber could have not only created the site, but also posted the "snitches get stitches" comment. The potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user leads to our conclusion that a printout of an image from such a site requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site in order to reflect that Ms. Barber was its creator and the author of the "snitches get stitches" language.

... In *Commonwealth v. Williams*, 456 Mass. 857 (2010), the Supreme Judicial Court of Massachusetts considered the admission, over the defendant's objection, of instant messages a witness had received "at her account atMySpace." *Id.* at 1171. In the case, the defendant was convicted of the shooting death of Izaah Tucker, as well as other offenses. The witness, Ashlei Noyes, testified that she had spent the evening of the

murder socializing with the defendant and that he had been carrying a handgun. She further testified that the defendant's brother had contacted her "four times on her MySpace account between February 9, 2007, and February 12, 2007," urging her "not to testify or to claim a lack of memory regarding the events of the night of the murder." *Id.* at 1172. At trial, Noyes testified that the defendant's brother, Jesse Williams, had a picture of himself on his MySpace account and that his MySpace screen name or pseudonym was "doit4it." She testified that she had received the messages from Williams, and the document printed from her MySpace account indicated that the messages were in fact sent by a user with the screen name "doit4it," depicting a picture of Williams. *Id.*

The Supreme Judicial Court of Massachusetts determined that there was an inadequate foundation laid to authenticate the MySpace messages, because the State failed to offer any evidence regarding who had access to the MySpace page and whether another author, other than Williams, could have virtually-penned the messages:

> Although it appears that the sender of the messages was using Williams's MySpace Web "page," there is no testimony (from Noyes or another) regarding how secure such a Web page is, who can access aMySpace Web page, whether codes are needed for such access, etc. Analogizing a MySpace [message] to a telephone call, a witness's testimony that he or she has received an incoming call from a person claiming to be "A," without more, is insufficient evidence to admit the call as a conversation with "A." Here, while the foundational testimony established that the messages were sent by someone with access to Williams's MySpace Web page, it did not identify the person who actually sent the communication. Nor was there expert testimony that no one other than Williams could communicate from that Web page. Testimony regarding the contents of the messages should not have been admitted.

Id. at 1172–73. The court emphasized that the State failed to demonstrate a sufficient connection between the messages printed from Williams's alleged MySpace account and Williams himself, with reference, for example, to Williams's use of an exclusive username and password to which only he had access. …

Similarly, in *People v. Lenihan,* 911 N.Y.S.2d 588 (Sup.Ct. 2010), Lenihan challenged his second degree murder conviction because he was not permitted to cross-examine two witnesses called by the State on the basis of photographs his mother had printed from MySpace, allegedly depicting the witnesses and the victim making hand gestures and wearing clothing that suggested an affiliation with the "Crips" gang. The trial judge precluded Lenihan from confronting the witnesses with the MySpace photographs, reasoning that "[i]n light of the ability to 'photo shop,' edit photographs on the computer," Lenihan could not adequately authenticate the photographs. *Id.* at 592. …

The State refers us, however, to *In the Interest of F.P.*, 878 A.2d 91 (Pa. Super. Ct. 2005), in which the Pennsylvania intermediate appellate court considered whether instant messages were properly authenticated pursuant to Pennsylvania Rule of Evidence 901(b)(4), providing that a document may be authenticated by distinctive characteristics or circumstantial evidence. In the case, involving an assault, the victim, Z.G., testified that the defendant had attacked him because he believed that Z.G. had stolen a DVD from him. The hearing judge, over defendant's objection, admitted instant messages from a user with the screen name "Icp4Life30" to and between "WHITEBOY Z 404." *Id.* at 94. Z.G. testified that his screen name was "WHITEBOY Z 404" and that he had printed the instant messages from his computer. In the transcript of the instant messages, moreover, Z.G. asked "who is this," and the defendant replied, using his first name. Throughout the transcripts, the defendant threatened Z.G. with physical violence because Z.G. "stole off [him]." *Id.* On appeal, the court determined that the instant

messages were properly authenticated through the testimony of Z.G. and also because "Icp4Life30" had referred to himself by first name, repeatedly accused Z.G. of stealing from him, and referenced the fact that Z.G. had told high school administrators about the threats, such that the instant messages contained distinctive characteristics and content linking them to the defendant. *In the Interest of F.P.* is unpersuasive in the context of a social networking site, because the authentication of instant messages by the recipient who identifies his own "distinctive characteristics" and his having received the messages, is distinguishable from the authentication of a profile and posting printed from MySpace, by one who is neither a creator nor user of the specific profile.

... It is clear, then, that the MySpace printout was a key component of the State's case; the error in the admission of its printout requires reversal.

In so doing, we should not be heard to suggest that printouts from social networking sites should never be admitted. Possible avenues to explore to properly authenticate a profile or posting printed from a social networking site, will, in all probability, continue to develop as the efforts to evidentially utilize information from the sites increases. A number of authentication opportunities come to mind, however.

The first, and perhaps most obvious method would be to ask the purported creator if she indeed created the profile and also if she added the posting in question, i.e. "[t]estimony of a witness with knowledge that the offered evidence is what it is claimed to be." Rule 5–901(b)(1). The second option may be to search the computer of the person who allegedly created the profile and posting and examine the computer's internet history and hard drive to determine whether that computer was used to originate the social networking profile and posting in question. ...

A third method may be to obtain information directly from the social networking website that links the establishment of the profile to the person who allegedly created it and also links the posting sought to be introduced to the person who initiated it. ...

Harrell, Judge, dissenting: ...

[A] reasonable juror could conclude, based on the presence on the MySpace profile of (1) a picture of a person appearing to Sergeant Cook to be Ms. Barber posing with the defendant, her boyfriend; (2) a birth date matching Ms. Barber's; (3) a description of the purported creator of the MySpace profile as being a twenty-three year old from Port Deposit; and (4) references to freeing "Boozy" (a nickname for the defendant), that the redacted printed pages of theMySpace profile contained information posted by Ms. Barber.

I am not unmindful of the Majority Opinion's analysis relating to the concern that someone other than Ms. Barber could access or create the account and post the threatening message. The record, however, suggests no motive to do so. The technological heebie jeebies discussed in the Majority Opinion go, in my opinion, however, not to the admissibility of the print-outs under Rule 5–901, but rather to the weight to be given the evidence by the trier of fact. ...

Questions

1. Do you think that Jessica Barber posted "SNITCHES GET STITCHES" to her MySpace page?

2. The MySpace profile in question contained a photograph of the witness (Jessica Barber) and the defendant (Antoine Griffin) embracing. Is there any serious doubt that the photo is authentic? If it is authentic, how can there any question about who wrote "SNITCHES GET STITCHES?"

3. Suppose that have just received an email claiming to be from the wife of a Nigerian diplomat, who is seeking your assistance in laundering several million dollars. Is it authentic? How would you tell? Now suppose that you have just received an email

claiming to be from your law school dean, inviting you to a reception in honor of a state supreme court justice. Is it authentic? How would you tell?

4. Imagine a contract dispute in which the interpretation of a key term depends on what the parties understood as they negotiated it. How would you authenticate an email message sent by your client to the opposing party? One sent to your client by the opposing party?

5. *Lenihan*, discussed in *Griffin*, holds that the possibility of Photoshopping means that an online photograph seemingly of an individual flashing gang signs is not sufficiently self-authenticating to show on its own that the individual actually flashed gang signs? Does this mean that authenticating a digital photograph now requires a chain of custody from the camera to a computer and including each additional computer it passes through? If so, most digital photographs are going to be inadmissible, aren't they?

6. Compare *Commonwealth v. Williams* and *In the Interest of F.P,* discussed in *Griffin*. Both involve the authentication of instant messages based on seemingly telltale details within the messages themselves. Are you convinced that the two cases are distinguishable? Which is closer to the facts in *Griffin*?

Romano v. Steelcase Inc.

907 N.Y.S.2d 650 (Sup. Ct. 2010)

Spinner, Judge:

Defendant Steelcase moves this court for an order granting said defendant access to plaintiff's current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information upon the grounds that plaintiff has placed certain information on these social networking sites which is believed to be inconsistent with her claims in this action concerning the extent and nature of her injuries, especially her claims for loss of enjoyment of life. ...

SCOPE OF PERMISSIBLE DISCOVERY

Pursuant to CPLR 3101, there shall be full disclosure of all nonprivileged matter which is material and necessary to the defense or prosecution of an action. To this end, trial courts have broad discretion in the supervision of discovery, and in determining what is "material and necessary" Within the context of discovery, "necessary" has been interpreted as meaning ""needful' and not indispensable" The "material and necessary" standard is to be interpreted liberally, requiring disclosure of "any facts bearing on the controversy which will assist preparation for trial by sharpening the issues and reducing delay and prolixity. The test is one of usefulness and reason." [*Allen v. Crowell-Collier Publ. Co.*, 21 N.Y. 2d 403, 406 (1968).]

Each discovery request is to be decided on a case-by-case basis, keeping in mind the strong public policy in favor of open disclosure. If the information sought is sufficiently related to the issues in litigation so as to make the effort to obtain it in preparation for trial reasonable, then discovery should be permitted. It is immaterial that the information sought may not be admissible at trial as pretrial discovery extends not only to proof that is admissible but also to matters that may lead to the disclosure of admissible proof.

INFORMATION SOUGHT FROM INTERNET SITES

Plaintiffs who place their physical condition in controversy may not shield from disclosure material which is necessary to the defense of the action. Accordingly, in an action seeking damages for personal injuries, discovery is generally permitted with respect to materials that may be relevant to both the issue of damages and the extent of a plaintiff's injury, including a plaintiff's claim for loss of enjoyment of life.

Thus, in *Sgambelluri v Recinos*, 192 Misc. 2d 777 (N.Y. Sup. Ct. 2002), an action arising out of a motor vehicle accident, the court held that plaintiff's wedding video taken two years after the incident was clearly relevant to the claim of permanency of injuries. As a result of the accident, plaintiff alleged that she sustained permanent injuries to her neck and back, and testified at her deposition that she can no longer participate in certain activities such as running or horseback riding. Defendant sought a copy of her wedding video on the basis that it might have shown plaintiff in various activities such as dancing, which would be relevant to the claims. Plaintiff objected on the basis of the personal nature of the video. The court decided in favor of disclosure, noting its relevancy to the claim of permanency of injuries. In so finding, the court reasoned that although the video is not a surveillance tape, as contemplated by CPLR 3101 (i), the statute's

> language [is] broad enough to encompass any film, photograph or videotape . . . involving a person referred to in paragraph one of subdivision (a), i.e., a party. This is consistent with the general policy of New York courts, allowing liberal disclosure. Moreover, the 1993 addition of subdivision (i) only strengthens the argument for open disclosure. (*Id.* at 779-780 [internal quotation marks omitted].)

Like the plaintiff in *Sgambelluri*, plaintiff herein also claims she sustained permanent injuries as a result of the incident and that she can no longer participate in certain activities or that these injuries have affected her enjoyment of life. However, contrary to plaintiff's claims, Steelcase contends that a review of the public portions of plaintiff's MySpace and Facebook pages reveals that she has an active lifestyle and has traveled to Florida and Pennsylvania during the time period she claims that her injuries prohibited such activity. In light of this, defendant sought to question plaintiff at her deposition regarding her MySpace and Facebook accounts, to no avail, and following those depositions, served plaintiff with a notice for discovery and inspection requesting, inter alia, "authorizations to obtain full access to and copies of Plaintiff's current and historical records/ information on her Facebook and MySpace accounts." Plaintiff has refused to provide the requested authorizations.

Both Facebook and MySpace are social networking sites where people can share information about their personal lives, including posting photographs and sharing information about what they are doing or thinking. Indeed, Facebook policy states that "it helps you share information with your friends and people around you," and that "Facebook is about sharing information with others." Likewise, MySpace is a "social networking service that allows Members to create unique personal profiles online in order to find and communicate with old and new friends" and is self-described as an "online community" where "you can share photos, journals and interests with your growing network of mutual friends," and as a "global lifestyle portal that reaches millions of people around the world." Both sites allow the user to set privacy levels to control with whom they share their information.

The information sought by defendant regarding plaintiff's Facebook and MySpace accounts is both material and necessary to the defense of this action and/or could lead to admissible evidence. In this regard, it appears that plaintiff's public profile page on Facebook shows her smiling happily in a photograph outside the confines of her home despite her claim that she has sustained permanent injuries and is largely confined to her house and bed. In light of the fact that the public portions of plaintiff's social networking sites contain material that is contrary to her claims and deposition testimony, there is a reasonable likelihood that the private portions of her sites may contain further evidence such as information with regard to her activities and enjoyment of life, all of which are material and relevant to the defense of this action. Preventing

defendant from accessing plaintiff's private postings on Facebook and MySpace would be in direct contravention to the liberal disclosure policy in New York State. ...

PLAINTIFF'S PRIVACY CONCERNS

Production of plaintiff's entries on her Facebook and MySpace accounts would not be violative of her right to privacy, and any such concerns are outweighed by defendant's need for the information.

Indeed, as neither Facebook nor MySpace guarantee complete privacy, plaintiff has no legitimate reasonable expectation of privacy. In this regard, MySpace warns users not to forget that their profiles and MySpace forums are public spaces, and Facebook's privacy policy set forth, inter alia, that "[y]ou post User Content . . . on the Site at your own risk. Although we allow you to set privacy options that limit access to your pages, please be aware that no security measures are perfect or impenetrable."

Further that

> [w]hen you use Facebook, certain information you post or share with third parties (e.g., a friend or someone in your network), such as personal information, comments, messages, photos, videos . . . may be shared with others in accordance with the privacy settings you select. All such sharing of information is done at your own risk. Please keep in mind that if you disclose personal information in your profile or when posting comments, messages, photos, videos, Marketplace listing or other items, this information may become publicly available.

Thus, when plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites, else they would cease to exist. Since plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy. As recently set forth by commentators regarding privacy and social networking sites: given the millions of users, [i]n this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking.

Further, defendant's need for access to the information outweighs any privacy concerns that may be voiced by plaintiff. Defendant has attempted to obtain the sought-after information via other means: e.g., via deposition and notice for discovery; however, these have proven to be inadequate since counsel has thwarted defendant's attempt to question plaintiff in this regard or to obtain authorizations from plaintiff for the release of this information. The materials, including photographs, contained on these sites may be relevant to the issue of damages and may disprove plaintiff's claims. Without access to these sites, defendant will be at a distinct disadvantage in defending this action.

Ordered, that defendant Steelcase's motion for an order granting said defendant access to plaintiff's current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information, is hereby granted in all respects; and it is further ordered, that, within 30 days from the date of service of a copy of this order, as directed herein below, plaintiff shall deliver to counsel for defendant Steelcase a properly executed consent and authorization as may be required by the operators of Facebook and MySpace, permitting said defendant to gain access to plaintiff's Facebook and MySpace records, including any records previously deleted or archived by said operators.

Questions

1. "If Romano has nothing to hide, she has nothing to fear from this discovery request." Do you agree? Why or why not?

2. This is a bit of an all-or-nothing result, isn't it? Assuming that Romano's Facebook profile has some relevant information, is there another procedure available that doesn't result in exposing her entire social life to the defendant?

3. Are you persuaded that Steelcase sufficiently established that the profile was likely to contain relevant evidence? Does a photograph of Romano "smiling happily in a photograph outside the confines of her home" sufficiently contradict her testimony that further discovery is warranted? Would the case have turned out differently if Romano had hidden her public profile entirely?

4. How do *Romano* and *Griffin* relate to each other? Is it possible that the same information about a party's online activity could be discoverable but inadmissible?

5. How would you advise a client who has a a social network profile? (How many of your clients are likely to have one?)

6. Could Steelcase's attorney have cut out the middleman and simply issued a friend request directly to Romano? Perhaps not. For one thing, lawyers are prohibited by ethical rules from communicating "about the subject of the representation" with other parties to a case; all contacts must be channeled through those parties' own lawyers. If your client were to tell you that she had received a friend request from opposing counsel, would you recommend she accept it? In light of your answer, should a Facebook friend request be considered a prohibited communication? May the lawyer read the other side's client's blog? If the lawyer has a blog, and knows that the other side's client reads it, must the lawyer stop posting about the case?

IV. Internet Technologies

This section provides a technical primer on the Internet. I have tried to emphasize the things that are important to know as you dive into the cases. As you read the fact section of an opinion, it may help to try to fit the court's discussions of the particular technologies at issue in a given case into the framework provided here.

The Internet

You may have heard of the metaphor of the Internet as a "cloud": big and opaque. In this section, we will systematically look inside the cloud to see how things work. What we will find may be less complex than you may have feared.

Networks and Protocols

Computer networks come in all shapes and sizes. There are networks between computers in the same room; there is a network that connects the International Space Station to earth. There are computer networks for cell phones, networks for playing video from your computer on your TV, even networks that connect a wireless mouse to your computer.

The key to every single one of these networks is the idea of a "protocol": a specification that describes how computers should use the network to communicate. You can think of a computer protocol as being like a diplomatic protocol: when two delegations meet, there is a precise order of formal greetings, handshakes, and statements. It may look bafflingly formal to an outsider, but the diplomats use it to communicate important information to each other about their countries' respective concerns.

Similarly, when two computers communicate, the protocol specifies every aspect of the technical process. A simple communications protocol along a cable might say, for example, that a message of binary 1s and 0s should be "encoded" as a series of electrical pulses of 500 nanoseconds each, with a 1 being a pulse at 1.5 volts and a 0 being a pulse at 1.5 volts. The sending computer turns the 1s and 0s into an electrical signal on the cable; the receiving computer looks at the voltage on the cable and turns it back into the 1s and 0s.

The enormous diversity of computer networks is possible because for each physical medium, there are different protocols designed to take advantage of that medium's characteristics. The idea is similar to the way that different kinds of roads have different traffic rules. You can drive faster on a highway than in a parking lot; you can drive different kinds of vehicles on a city street than on a bicycle path; you drive on the right side of the road in some countries and the left side in others.

It is common to call a physical medium connecting two computers together with an appropriate protocol a "network link." Here are some common (and less common) network links:

- Ethernet is a widely used protocol for local-area networking (e.g., within a building, rather than cross-country). Its physical medium is most often "category 5 cable," a set of plastic-wrapped wires with a phone-like plug at each end. The Ethernet protocol specifies how computers connected by an Ethernet cable should "talk" by turning the information they want to send to each other into electrical pulses, how quickly they can talk, and what to do if two of them start talking at the same time.
- Many computers use WiFi for their local-area networks. Here, the physical medium is the atmosphere itself. Each computer using WiFi has a small radio transmitter/receiver. The WiFi protocol tells the radio transmitter on what frequencies

to broadcast and listen, how loudly and for how long to transmit, and what to do if someone else starts transmitting at the same time.[*]

- Your cell phone also contains a radio, as do cell phone towers. Again, the physical medium is the atmosphere. Instead of using WiFi frequencies and transmission rules, however, the phones and towers use protocols with names like EDGE, EVDO, and UMTS to specify how they should transmit information to each other.
- Internet signals can be carried over traditional copper or modern fiber-optic phone cables; the DSL and GPON standards, respectively, provide protocols for doing so. Cable companies use DOCSIS to do the same over cable connections. If you remember dialup, it used the PPP protocol to provide Internet access by having your computer make a phone call to a local phone number, and encoded the data transmissions as audio (which is why picking up another extension and making noise would generally destroy the connection).
- Fiber-optic "backbones" provide long-distance connections on land and via undersea cable. They are engineered for super-high transmission speeds, using highly specialized protocols .
- Computer data can even be transmitted via carrier pigeon. Here, the pigeon is the physical layer, and the protocol specifies that data should be transmitted by writing digits on a piece of paper wrapped around the pigeon's leg and secured with duct tape.[†]

Inter-Networking and the Internet Protocol

The next complication is that not every computer is on the same small local network. Your computer has a direct network connection to only one or a few others. The overwhelming majority of computers in the world do not have direct connections to each other, and it would obviously be impossible to try. How do we use the diverse networks we have in order to build up something like the Internet, where it is possible for computers around the world to communicate? This is the problem of inter-networking, and the answer lies in something called the Internet Protocol, or IP.

The first key idea of IP is "routing." Suppose that you want to download an MP3 from Amazon's MP3 store. There isn't a wire that directly connects your computer to Amazon's computer. Instead, the information making up the MP3 is passed along from one computer to another – computers that *are* directly connected (by a wire or other network link) – until it reaches you. In essence, Amazon's computer hands off the MP3 to a computer that is connected to it and is slightly closer to you. That second computer hands off the MP3 to a third, which hands it off to a fourth, and so on until it is handed off to a computer that is directly connected to yours, which hands it off to you. Computers that participate in the process are generally called "routers."

Each handoff is, in essence, a computer-to-computer copy. The computer making the handoff transmits a complete copy of the data in the file to the next one. As soon as the receiving computer acknowledges that it has received all the data, the sending computer knows that it can delete its own copy. Transmitting information through the Internet thus requires making as many transient intermediate copies as there are computers in the chain from the original sender to the final recipient.

Along the way, the data will travel over many different kinds of network links. It might start out on Ethernet inside Amazon's data center, then be transmitted along

---

[*] Thus, a standard wireless router is a device that has both a WiFi-compatible radio and an Ethernet-compatible jack. It translates messages that come in along the Ethernet link into WiFi radio signals, and vice-versa.

[†] No kidding. *See* D. Waitzman, *A Standard for the Transmission of IP Datagrams on Avian Carriers* (1990) (RFC 1149), http://tools.ietf.org/html/rfc1149.

backbone links until it reaches your local area, then travel on a fiber-optic cable supplied by your phone company, and finally reach your computer via WiFi inside your home. All of these network links have one thing in common: they can be used to carry IP messages.

This is a truly profound idea. Network engineers would say that IP is "layered" on top of these various network links. The goal of any of the lower-level link protocols listed above is to create a network that is capable of carrying IP messages. Once that is accomplished, the IP message can be carried from computer to computer across multiple different networks: Ethernet, backbone, WiFi, etc. The message itself does not change in any significant way, even though the different link protocols will encode it in radically different ways on different networks.

This is why IP is called the *Inter*-net Protocol. It is designed to enable *inter*-networking: the tying together of different networks. IP plays the crucial role of giving these diverse networks a single common technical language. Indeed, this is where the *Inter*-net gets its name: it was an experiment in inter-networking that was so wildly successful that it became "the" Internet rather than just "an" Internet.

Routing and Addressing

But how do the computers along the chain know *where* to send the data? They may only be connected to a few other computers, but the data could potentially be going to any of the billions of computers on the Internet. How do they decide which of their neighbors to pass the data along to?

The answer is that each computer on the Internet has a unique "address," called an "IP address" (named after IP, of course). An IP address is a 32-digit binary number; by convention, they are written as four decimal numbers separated by periods. For example, here are the IP addresses of a few well-known computers:

- apple.com: 17.172.224.47
- google.com: 74.125.91.99
- nytimes.com: 199.239.136.200
- mit.edu 18.9.22.69

Every message is carried in the electronic equivalent of an envelope with the IP address of its destination stamped on the outside. When a router receives a message, it examines the IP address on the message. If that IP address is the router's own address, then the message has reached its destination and the process is done. Otherwise, the router examines a large database called called a "routing table," which tells the router, what the next intermediate destination should be for any possible ultimate destination. For example, a router's routing table might say that all messages for google.com and apple.com (which are on the West Coast) should be given next to its neighbor A, but that messages for nytimes.com and mit.edu (which are on the East Coast) should be given to its neighbor B.

Each router has its own routing table. The process of constructing them is one of the most complicated and intricate aspects of keeping the Internet functioning. At a high level of generality, what happens is that individual routers tell each other what computers they know how to get messages to. The information gradually propagates throughout the Internet, until – in theory – every computer knows how to reach every other computer.

Packet-Switching

The next complication is that most messages are too big to send all at once in this fashion. Instead, they are broken down into smaller "packets" (sometimes also called "datagrams"). Each packet is sent separately, like a jigsaw puzzle that is broken down into individual pieces, each of which is sent in a separate envelope to the same destination. Along the way, they may travel by different routes, depending on factors like

temporary congestion in some parts of the Internet, or routers coming on- or off-line and thus becoming available or unavailable to pass packets along.

Packet switching may seem counterintuitive, but it has some notable advantages. One is that it is much more efficient than the alternative of "circuit-switching," i.e., holding a dedicated connection all the way from sender to recipient open for the entire duration of the transmission. Circuit-switching commits to a single chain of computers from source to destination, but packet-switching allows the transmission to respond to moment-to-moment changes in the Internet, taking advantage of faster routes and avoiding sudden traffic jams. Packet-switching also avoids tying up the intermediate computers when there is no data flowing; think of a streaming concert video, where the flow of information will last for hours, but is much less than the full capacity of any of the routers along the way. In addition, as we will see shortly, packet-switching can be very resilient to errors.

These three big ideas – routing, addressing, and packet-switching – collectively characterize the Internet Protocol. As its name suggests, IP is central to how the Internet works. Indeed, "the global network in which computers communicate using IP" comes very close to being *the* technical definition of the Internet. We will see throughout the this book how these technical features have important consequences for the law.

Reliable Transport

IP is not the only protocol that matters on the Internet. Instead, network engineers commonly speak of a "protocol stack" of multiple protocols in use at one time. The "stack" metaphor captures the idea that these protocols are layered: ones at higher levels take advantage of the services offered by the ones at lower levels to do their jobs. Here is a simplified view of the protocol stack used by a typical home computer:

- Application (e.g. email, web, etc.)
- Transport (TCP)
- Network (IP)
- Link (Ethernet)
- Physical (category 5 cable)

We started off by discussing the physical and link layers. Then we saw how the network layer – IP – ties different networks together into a single Internet with world-wide addressing and routing. Now it is time to move up again.

The next layer above IP in the protocol stack is the transport layer, and the most common protocol there is TCP, the "Transmission Control Protocol."[*] It has several jobs, but the most significant is "reliable transport": that is, making sure that every piece of a message reaches the destination. IP is a so-called "best efforts" protocol; routers will do their best to make sure that packets get where they should, but they make no promises. Bad stuff regularly happens that causes packets to be lost. Sometimes a router is congested, with too much incoming traffic, and it needs to start "dropping" packets in order to cope, like an overworked mail carrier tossing some envelopes in the river. At other times, transient conditions, like electrical interference or a bug in a router's software, can cause a packet to be scrambled so badly that the data in it is unrecoverable.

---

[*] TCP is not the only transport protocol. Not every application needs to ensure that every single packet is delivered. A live voice chat, for example, is better off letting the audio cut out for a fraction of a second than waiting for seconds for every last bit to arrive. Multiplayer video games often prefer to minimize transmission delay so that players can respond more quickly to each other. These and other applications often use their own, specialized transport protocols. They have in common with TCP and with each other that they all depend on IP: each of them uses IP to transmit its packets, they just do different things with the results.

TCP deals with all of these problems through good bookkeeping. The sender and the receiver each maintain a list of the individual packets making up a transmission. As the receiver receives each packet, it checks off that packet on its list and informs the sender that it has. If the receiver realizes that it is missing a packet – for example, because it is receiving more recent packets without having received an older one – it asks the sender to "retransmit" the missing packet. Meanwhile, the sender is keeping track of which packets the receiver has acknowledged. If too long a time passes without an acknowledgment from the receiver, the sender assumes that something has gone wrong and initiates retransmission on its own.

This is why packet-switching can be surprisingly more error-resistant than sending an entire message at once. It is true that, as with a jigsaw puzzle split among ten thousand envelopes, there are more ways for something to go wrong. But if a few packets go missing, TCP sees to it that just the missing ones are retransmitted, rather than needing to start the entire message from scratch. To continue the analogy, if a few puzzle pieces are missing, it's easier to resend just the missing ones than to mail the entire puzzle again. Similarly, because the packets are smaller, they are less likely to suffer an error than a larger message would be. A single jigsaw piece can be mailed in an ordinary envelope; the entire assembled puzzle will require a special oversize padded mailer.

TCP is also responsible for "flow control": the process of determining how fast the sender slings packets through the Internet toward the receiver. If you have a good fiber-optic connection, you would obviously prefer to send packets faster than if you are connecting through a slow satellite connection. Put another way, TCP automatically adapts on the fly to the amount of available "bandwidth" between sender and receiver. (The actual algorithms it uses to do so all involve clever communication between sender and receiver, and have been tuned over the years to values that seem to work well.)

Here, we can see another advantage of layering. TCP can completely ignore the details of the underlying network. It doesn't need to know whether its running on a WiFi network or on Ethernet or whatever. It can delegate all of those details – along with the details of routing – to lower-layer protocols. TCP is only responsible for reliable transport and flow control, so it can focus on doing its job well. Unsurprisingly, this helps make TCP simpler than if it also had to do all of these other jobs. Computer programmers would say that layering is a kind of "modularity": separating out different functions into smaller pieces makes them easier to get right.

Applications

At last we arrive at the part of the Internet you are probably most familiar with: applications. These are the programs that actually do things, like email, web browsing, and instant messaging. They use TCP/IP[*] and other lower-level protocols to move data back and forth, and then do interesting things with it.

The first important detail here – one you are likely already familiar with – is the idea of clients and servers. A server is a computer that has a particular resource or that does a particular job. For example, the computer that stores your law school's webpage is a sever, unsurprisingly called a "web server." Other common servers you probably use on a regular basis include email servers like Yahoo! Mail and your school's email, e-commerce servers like the iTunes Music Store, and chat servers that tell you whether your friends are online.

A client is a computer that connects to a server to get information or have the server do something for it. If you look at your law school's webpage, your computer is the client. It sends a message over the Internet to the web server, asking for the webpage; the server responds with a message that contains all the information making up the

[*] The two were designed simultaneously and are so frequently used together that they often go by this combined acronym.

webpage. The process is similar with other servers. By convention, information that goes from a client to a server is "uploaded"; information that goes the other way, from server to client, is "downloaded."

Applications often have their own protocols, layered on top of TCP/IP and the other lower-level protocols. When one computer sends an email to another, it uses a protocol named SMTP to tell the receiving computer whom the message is from, whom it is for, what its subject is, and what its contents are. BitTorrent is a publicly published protocol for exchanging complete files. Skype uses a secret protocol to exchange voice messages. Games use their own protocols to update players' computers on what everyone else is doing.

The Web

Perhaps the single most important application on the Internet today is the World Wide Web or "web." The web actually consists of two closely related standards. The first is a protocol, the Hypertext Transfer Protocol (or "HTTP"), for sending webpages from servers to clients. The second is a format, the Hypertext Markup Language (or "HTML") for describing a rich display with images, hyperlinks, and interactivity using nothing but raw text.

Let us start by considering the process of obtaining a webpage from a server. Your web browser (e.g. Internet Explorer, Firefox, Chrome, or Safari) is a program designed to request web pages from servers and display the results. Suppose, for example, that you want to read the latest technology headlines from the New York Times, so you type "nytimes.com" into the the address bar of your browser. It uses TCP to send a message to the New York Times server at nytimes.com. In response, the New York Times server will send back a message containing the webpage itself. The rules of the road for this process – e.g., how the client describes the web page it wants, and how the server explains whether that web page is available or not – are governed by HTTP. If you have ever seen a webpage that displays the message "Error 404 not found," then you have seen HTTP at work. 404 is the error code used by HTTP to signal that the webpage the client asked for does not exist.

What you have obtained from the server is not yet a webpage, only a long text file, You can examine the details by going to any webpage and selecting the "View Source" command in your browser.[*] What you will see is a set of instructions for displaying the webpage you are looking at. This is the actual, literal data that was sent from the server to your computer; your web browser is then able to read the data transform it into the webpage you see. (When people talk about "the source" of a webpage or "the HTML" for the page, this is what they are referring to.)

Try this, for example, at your favorite news site or blog. Pick a headline, and then try to find it in the page's source. You should be able to pick it out, along with a lot of things between angle brackets, i.e. "<" and ">" called "tags." These tags are the instructions, which your browser turns into visible formatting in the webpage it displays to you.[†] Here is some simple HTML:

---

[*] In most browsers, this is available under the "View" menu.

[†] Not every tag has visible consequences. In Chapter 7, you will encounter "meta tags," which carry information about the page (intended to be used by search engines), and which are not ordinarily shown to normal web users. You can inspect them, however, by using the View Source command.

```
<li>I agree. We <b>have</b> been here before, as the <a
href="http://nytimes.com">New York Times</a> recognizes.</li>
```

When displayed by your browser, this text will look more like this:

- I agree. We **have** been here before, as the New York Times recognizes.

What's different between the source and the displayed version? First, the <li> tag, which stands for "list item," tells your browser that what follows should be formatted as a bulleted item in a list. The matching tag (which has a slash before the li) marks the end of the item. Second, the tag tells your browser to format the following text as bold, up until the matching tag marks the end of the boldface segment. And third, the <a> tag, or "anchor" specifies that the following text is a hyperlink. If you click on it, your browser loads the web page it points at, in this case the New York Times's homepage. How did your browser know which new webpage to load? It uses the location specified inside the <a> tag, following the "href"[*] – in this case, "http://nytimes.com".

One last HTML tag is worth explaining: <img>. Here is an example:

```
Yes, I've seen it, but I have no idea where they got the name
from: <img src="http://james.grimmelmann.net/images/grimmelman-
mosaic.jpg"/>
```

This will turn into the following in a browser:

Yes, I've seen it, but I have no idea where they got the name from:

Here, the <img> tag tells the browser that it should display a particular image in that position. The image isn't sent as part of the webpage itself. Instead, your browser, when it sees an <img> tag, sends an additional request to the server with the image. (Here, that server is james.grimmelmann.net, and note that the server where the image comes from need not be the same server as the one where the webpage came from.) The browser then drops the image into the place on the page where the <img> tag was. You can think of the tag as being a kind of placeholder for the image, one that includes instructions for how to fill in the place with a specific image.

The Domain-Name System

One more application is especially important to the functioning of the Internet. The domain-name system converts human-readable names (like "google.com" and "icanhascheezburger.com") into the IP addresses used by computers.

[*] "href" is a less obvious abbreviation than some of the others; it is short for "hypertext reference."

When you look up a domain name – say, my.nyls.edu – what really happens? The process works hierarchically, from right to to left. Any URL, such as http://my.nyls.edu/cp/home/loginf, can be broken down into three parts. The http:// at the start is a protocol identifier, which indicates that this is a request for a web page. The my.nyls.edu in the middle – everything up through the next slash – is the domain name that identifies the server from which you're requesting the web page. And the "cp/home/loginf" part (everything following the slash) identifies to the server which particular page you are asking for.

The general rule is that if your computer (e.g, your web browser, when you type a URL into the address bar) asks a domain-name server to look up a domain name, it will tell you the IP address of the computer with that domain name if the server knows. If the domain-name server doesn't know about that particular domain name, the server will give you the IP address of another domain-name server that can help you. That is, it will either help you or respond with the technical equivalent of "I don't know, but here's someone who might." Here's a simplified example:

(1) You start by asking the "root name server" what it knows about my.nyls.edu. The root name server "understands" the last part of the address, here my.nyls.**edu**. It tells you that another computer – the so-called "top-level domain (TLD) name server" for all ".edu" sites worldwide – can help, and gives you the IP address for the TLD name server.

(2) You ask the TLD name server for .edu what it knows about my.nyls.edu. This server "understands" the second part of the address, here my.**nyls**.edu. It tells you that another computer – the name server for nyls.edu – can help, and gives you the IP address of this other name server.

(3) You ask the name server for nyls.edu what it knows about my.nyls.edu. This server "understands" the third part of the address, here **my**.nyls.edu. It gives you the IP address for my.nyls.edu directly. Armed with the IP address, your computer can now directly contact my.nyls.edu.

This process could in theory be iterated repeatedly, although in practice it rarely continues for more than a few steps.

Internet Applications Problem

Familiarize yourself with the following:

- Jason Kottke's blog
- Your email service
- Amazon.com
- AIM (AOL Instant Messenger)
- Skype
- World of Warcraft
- Twitter
- YouTube

You don't need to sign up for accounts or to use these applications, but you should be at least passingly familiar with them. They provide a useful range of examples. Do your best to answer the following questions for each of these applications:

(1) What can you do using this application?

(2) Does the application require that you and other users both be online at the same time? If so, how does the application figure out that you're both available?

(3) How does the message get from your computer to someone else's (or vice-versa)? Is it stored anywhere along the way? Who could listen in or read it if they wanted?

(4) How – in a very general sense – is the content encoded? Is it human-legible? Does its quality suffer in transit?

(5) Are there servers somewhere that assist in making the application available? If so, do they store the content, or do they merely assist in making connections? Could you make connections without the assistance of a server? Who's in charge of keeping those servers running, providing them with electricity, and so on?

(6) Do you need an account to post content? To receive it? How much information about yourself do you need to give up in order to participate?

(7) Who's allowed to post content, and of what sort? Is this an egalitarian medium, or one in which only a few people speak and the vast majority only listen?

(8) What happens "under the hood?" Is there a flow of information that you can describe in general terms, or does something so mysterious happen that it might as well be magic?