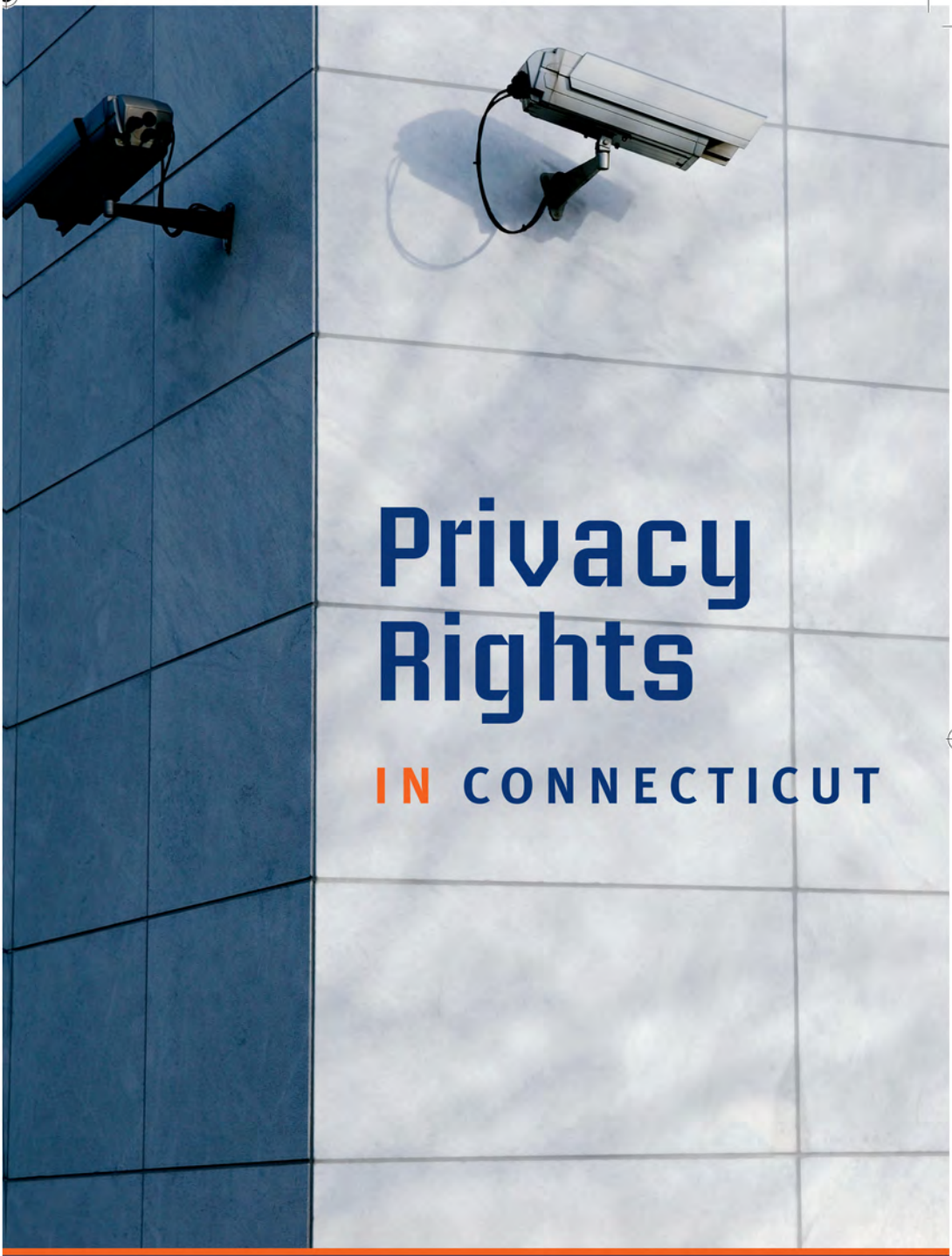

Privacy Rights

IN CONNECTICUT

ACLU
AMERICAN CIVIL LIBERTIES UNION of CONNECTICUT

Privacy Rights in Connecticut

A guide by the American Civil Liberties Union of Connecticut

Robert Schultz, a volunteer attorney with the American Civil Liberties Union Foundation of Connecticut, researched and wrote this guide with supervision and editing by Sandra Staub. Jeanne Leblanc also edited and David McGuire reviewed and provided research support. Other volunteers, including Luke Stankiewicz and Anna Keegan, provided research support. EberleArts designed the cover.

For online updates to this guide please visit www.acluct.org/privacy

American Civil Liberties Union of Connecticut
330 Main St., First Floor
Hartford, CT 06106
860-523-9146
www.acluct.org

INTRODUCTION

It's often said that the modern right to privacy originated in 1890 when Louis Brandeis and Samuel Warren argued in a now famous law-review article that privacy is an essential aspect of the rights to life, property, and the right "to be let alone."[1] Especially concerned with journalists and their aggressive use of photography, the authors asserted that press and other intrusions should give rise to a cause of action for "invasion of privacy."[2] And their arguments resonated, prompting courts and legislatures to develop just such a body of law.[3] But their article, and the laws it inspired, addressed rights enforceable principally against other individuals, companies, and the press.[4]

Privacy from government intrusion is a whole different matter, and it has been governed primarily by provisions to protect privacy under another name. These include the Fourth Amendment to the Constitution of the United States and Article 1, Section 7 of the Constitution of the State of Connecticut (originally Article 1, Section 8 of the 1818 Constitution), forbidding unreasonable searches and seizures.[5] Although neither explicitly mentions privacy, courts applying these provisions eventually began to ask whether the government had invaded a person's actual and reasonable expectation of privacy.[6] And, gradually, the Supreme Court of the United States came to understand that privacy so underlies other rights in the Constitution that, even though the word isn't used, privacy itself must be a freestanding right that governments may not abuse.[7]

So there is no doubt that we all have certain legally enforceable rights to privacy, but the scope of these rights is anything but clear. That's because rights to privacy have always existed in tension with free speech, legitimate law enforcement needs and, most urgently, technology.

Never has the conflict between privacy and technology been tenser than now. Rather than merely worrying about print newspapers as Brandeis and Warren did or about physical searches as the Framers did, we must daily face the highest-tech potential intrusions into our lives. Private and public security cameras, sometimes with facial recognition software, can track our every move.[8] Police scan our

license plates to learn where we travel.[9] Private corporations note our whereabouts from our cell phones, sometimes sharing that data with police.[10] And practically anybody can perpetually monitor our personal relationships, buying, searching, and reading on the internet and its social media.[11]

What's worse, while the ways of watching us and searching our things have become more powerful, so have the computers that permit storage and pooling of the data collected. Those computers are now so large that they allow essentially indefinite retention of all information ever collected.[12] And the search programs to govern such databases have likewise improved,[13] so that all the data ever gathered may be at once analyzed. Nor is that the end: the internet already does, and its increasingly advanced successors will, facilitate practically instantaneous and indelible disclosure. Thus high-tech snooping is ever likelier to reveal each one of us and our secrets to everyone.

Despite these rising threats to individual privacy, the law has lagged behind. Legislatures have been slow to recognize the changes in technology and adapt statutes to maximize the protection of individual privacy.[14] And judges are struggling to fit constitutional protections or common-law rights to a contemporary expectation of privacy in light of realities they may not fully understand.[15] All this has resulted in gaps. For example, the law doesn't address long-term aggregation of information because, under those eighteenth- and nineteenth-century regimes, there's little protection for what's collected in public view, and no thought of how computers might indefinitely store it. Yet even data collected in public view, if it's kept long enough, might be used to draw a picture of an individual's habits and associations. And that itself might mark a fundamental change in privacy as we've so far known it.

Goals of this publication

Building on the 2003 edition of *Privacy Rights in Connecticut* by the American Civil Liberties Union of Connecticut, this guide identifies issues relevant to the privacy of any person living in Connecticut and explains the relevant laws.[16] Those laws will include federal and state constitutions, federal and state statutes,

state common-law torts (or judge-made laws), and contracts. But we won't limit ourselves to describing the current state of privacy law. Instead, we'll identify the areas where we think that the law has fallen behind, as with the aggregation example we just mentioned. By discussing this and other gaps in the law, we hope to participate in the debate on how best to formulate contemporary privacy protection in a comprehensive and prospective statutory scheme to reinvigorate our expectations of privacy and provide remedies.

As with any legal guide, this handbook is no substitute for speaking to a lawyer if you have a problem. For one thing, the law is always changing; for another, we can't address directly the nuances of every law, much less every case.

GENERAL PRINCIPLES AND SOURCES OF LAW

While speaking of Privacy Laws, we're actually discussing a vast and disparate body of law. Indeed, given the variety of law and the breadth of the topic, there's no practical way to explore it all except by taking each individual subtopic in turn. So we've organized this guide by subject matter. Certain general principles will recur, so we explore them at the outset.

Federal and state constitutional law

When people think of fundamental rights such as privacy, they often think of the Constitution of the United States, presuming that it will protect them from other individuals. But the federal Constitution—with irrelevant exception—doesn't apply to private individuals or companies, but only the government.[17] That's true of the Constitution of the State of Connecticut, too.[18] So you can't press a constitutional claim against your neighbor, your boss, or the corporations that run the technology that's tracking your internet use. Those will be addressed by the other laws, explained below.

The Fourth Amendment to the Constitution of the United States

The most important privacy-related provision in the Constitution of the United States is the Fourth Amendment, which secures our right against unreasonable searches and seizures. (Originally, that amendment was written to apply only to the federal government, but, by way of the Fourteenth Amendment enacted after the Civil War, it now binds all state governments, too.[19]) It reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[20]

Because this provision forbids "unreasonable searches and seizures," it has no bearing unless there's been a search or a seizure.[21] So the threshold question is whether the police have conducted a search (we'll focus on searches rather than seizures). Unfortunately,

that's not as clear-cut as you might hope, though it's not without its standards.

As explained in the 2012 case of *United States v. Jones* and reiterated in this year's *Florida v. Jardines*, there are two tests that the Supreme Court of the United States applies to decide whether a search occurs.[22] The first asks simply whether authorities seeking evidence have trespassed on your person, house (including the curtilage, or area immediately around it like your front porch), papers, or effects.[23] To be sure, not every trespass on your property to gather evidence is a search, for the Fourth Amendment's trespass test applies only to the enumerated items: persons, houses, papers, effects and not, for example, to "open fields."[24]

The second test, supplementing the first, asks a two-part question: whether the police have invaded your (1) actual and (2) reasonable expectation of privacy.[25] In other words, to conduct a search, police must intrude on something that you are in fact trying to keep private, and the way you're trying to keep it private must be one that society generally accepts.[26]

Some examples will show how these tests work together. Imagine, for example, that the police suspect that you're growing marijuana and come to your house. (We use this example because so many cases actually involve police looking for marijuana plants.[27]) They may walk up to your door, knock, and even ask questions hoping you'll give yourself away, but they may not step onto the front porch uninvited if they intend to uncover evidence and possess the means to do so, like a drug-sniffing dog.[28] That's because that's a trespass, just as it would be if they barged in without your permission and looked into your closets for ultraviolet lights and marijuana plants. Consequently, when the police commit such a trespass to gather evidence, they've conducted a search. Of course in many cases a trespass involving the home would also be an invasion of a reasonable expectation of privacy, but the Court has held that, if it finds a trespass under the Fourth Amendment, it doesn't need to apply the second test.[29]

But what if police walk along the street in front of your house and happen to see marijuana growing in your yard or on display in

your window, or if they happen to look through the window of your car and see drugs on the seat, where everyone can see them?[30] What if they fly over your house and see marijuana growing in a field in back?[31] In those cases, there's no search.[32] First, there's no trespass because the police have gone only where they're allowed to go, and, second, even if you wanted to keep the plants private, there's no reasonable expectation of privacy because the police could see the plants from where anyone might legally go and see them, so you'd be foolish (says the Court) to think them secret.[33] Such is the case, too, if the police watch your home from a public place to see you come and go, and even follow your car—because anyone can legally use the streets and see you use them.[34]

What if they walk past your house to a path behind it that leads them past no-trespassing signs to a fence that they look over to see, in the open field beyond it, marijuana growing?[35] That's a trespass, but, as we've said, not every trespass constitutes a Fourth Amendment violation, certainly not one in open fields.[36] Moreover, there's no reasonable expectation of privacy for what grows in open fields that can't be protected from intrusion.

So in the interplay of these tests there may be a trespass without an invasion of your expectation of privacy, but the converse is true, too: there may be an intrusion upon your reasonable expectation of privacy without a trespass. The case that gave rise to the two-prong expectation of privacy test is a good example. There, Charles Katz went to a phone booth, closed the door, and spoke to someone on the phone as police from a distance used a microphone to eavesdrop on Katz's half of the call.[37] There was no trespass, no physical intrusion on his person, papers, home, or effects or any property of any kind. Nevertheless the police had conducted a search.[38] That's because Katz demonstrated by closing the door that he actually expected the conversation to be private and, as important, he was reasonable to think it would be private—that is, society generally would agree with him.[39] (Actually, this statement of the test was written by concurring Justice Harlan and didn't become the law until a majority of the Court later adopted his view as its own.[40]) In this way, the two-prong expectation-of-privacy test may provide greater protection than the trespass test alone.

We hope that these examples give a good sense of what's a search and what isn't. But we'll have to ask you to bear with us for just one more example because it will become important later in our discussion. Suppose the police think that you're selling the marijuana you grow and want to see if you've made deposits in your bank. It's not a search, the Court has ruled, to go to the bank and demand your financial records.[41] That's because you've already shared those financial records with the bank, a third-party, and they're not confidential but commercial, so you can't claim that you have an expectation in their privacy.[42] (Congress tempered this ruling by enacting the Right to Financial Privacy Act of 1978 to give customers rights to notice and the opportunity to contest government subpoenas in certain cases.[43]) Of course the result would be the opposite if the police learned the same information by rifling through your papers.

So that's the threshold, anyway. The next question comes only when there has been a search, and it's whether that search was reasonable. The general rule is that every warrantless search is presumptively unreasonable,[44] especially when authorities enter a home.[45] Therefore, before conducting a search, police usually must obtain a warrant from a neutral third party, in other words a court (the cases often say magistrate), instead of an officer charged with investigating crime.[46] The warrant will issue only when the court is presented with enough information under oath or affirmation to persuade a reasonable person that the search would uncover evidence of a crime in a certain place—or, that is, on a showing of probable cause.[47] And the warrant must state with particularity where the police will search, and what or whom they will look for or seize.[48] That said, exceptions to the warrant requirement have grown over the years, and are now many. We'll talk about the two main exceptions here.

The first is consent to the search. Consenting to have your things searched doesn't mean that you've given up your actual expectation of privacy such that there's no search at all; it simply means that the search is reasonable.[49] But, because the police have lots of power, the question of whether you're really acting voluntarily when you consent can be a complicated one.[50] Further complicating the analysis

are the Court's holdings that a third-party may give consent, such as when a wife hands the police her husband's things or a person whom police reasonably believe lives in a dwelling lets them in.[51]

The next exception (for now) to the warrant requirement is for emergencies, when there isn't enough time to get the warrant.[52] That's fair enough. After all, some people run away and some evidence doesn't last for long or might get destroyed while police wait for a court to issue the warrant.[53] Whether there's an exigency justifying an exception to the warrant requirement depends on the facts of each case, and the Supreme Court has refused to adopt categorical rules, most recently rejecting a state's argument that dissipation of alcohol in a drunk driver's blood is always an emergency justifying a warrantless search.[54] Even where there's an exigency there generally must be probable cause to justify the search—that is, enough to persuade a reasonable person that the search will uncover evidence associated with a crime.[55] Nor should the search exceed what's necessary to find the relevant things,[56] though police conducting one legal search and happening upon something that they didn't expect in plain view may respond accordingly.[57]

But the probable cause requirement doesn't apply to all searches. Indeed, the Fourth Amendment by its terms requires that searches be *reasonable* rather than explicitly requiring probable cause (the probable cause requirement applies directly to warrants rather than searches).[58] Consequently police may sometimes stop you and conduct a limited search, or frisk, of your person even without probable cause.[59] This is called a *Terry* stop and frisk, from a case of the same name.[60] In such a case, police need only reasonable suspicion based on specific, articulable facts to believe that a person is armed and dangerous, for example.[61] In *Terry* itself, that reasonable suspicion was based on a policeman's observation of a man pacing back and forth and staring into a store window with another man until they were joined by a third, furtively conferring as if they intended to rob the store.[62] The Court said any cop with any sense would be worried by that and, moreover, concerned that Terry might be armed.[63] (If all these rules aren't confusing enough there are other searches—called special-needs and administrative searches—that don't require any individualized suspicion at all; but

we'll save them for the last section of this publication, *Privacy in Our Persons*.)

Now let's turn to the final question about the Fourth Amendment: what happens if the search is unreasonable? Then, of course, there's a violation of the Fourth Amendment and—generally speaking—the evidence from the unreasonable search is suppressed, which means that it may not be used at trial against the person whose rights are violated.[64] This is called the "exclusionary rule."[65] The rule sometimes applies to evidence found as a proximate consequence of the illegal search (and which wouldn't have been found anyway).[66] That's called "the fruit of the poisonous tree."[67] The exclusionary rule is meant to deter misconduct by police, who are engaged in "the often competitive enterprise of ferreting out crime."[68] Also, a person whose Fourth Amendment rights have been violated may sue an employee of the government who violated them, such as a police officer.[69] To be clear, we believe a person whose constitutional rights are violated may sue for what damages flow naturally from the violation, but the U.S. Court of Appeals for the Second Circuit—whose opinions are binding on federal courts in the region where Connecticut lies—says a plaintiff generally may not recover damages for a conviction and imprisonment resulting from illegally seized evidence when a judge made an informed decision not to apply the fruit-of-the-poisonous-tree doctrine.[70]

Constitution of the State of Connecticut, Article 1, Section 7

So far, we've discussed only federal law. But the Constitution of the State of Connecticut has its own provision to protect against unreasonable searches and seizures. It's Article 1, Section 7 (it was section 8 in Connecticut's 1818 constitution). It reads:

> The people shall be secure in their persons, houses, papers and possessions from unreasonable searches or seizures; and no warrant to search any place, or to seize any person or things, shall issue without describing them as nearly as may be, nor without probable cause supported by oath or affirmation.[71]

Because this provision is a state law, the Supreme Court of the United States may not determine its scope. Instead, the Connecticut Supreme Court has the final say, and it may depart from the Supreme

Court of the United States to provide more protection for people in Connecticut than they'd get from the federal Constitution alone, although it can't take any away.[72] (This extra protection generally applies only in state courts and not to federal prosecutions in federal court.[73])

It has not been very often that the state Supreme Court has held that Article 1, Section 7 provides greater protection than the Fourth Amendment.[74] That's largely because of the similarity between the two provisions.[75] And the state analysis is generally the same as the federal one: whether the police have invaded your actual and reasonable expectation of privacy.[76] Other major analytical approaches are mostly the same, too: for example, the state Constitution permits *Terry* stops and frisks.[77] So we'll separate the state amendment from the federal amendment only as necessary.

Federal constitutional right to privacy

The federal right to privacy was first articulated when the Supreme Court of the United States struck down a Connecticut statute banning all contraception.[78] In that case, the Court reasoned that, even though the federal Constitution does not include the word privacy, it contains several provisions to guarantee privacy rights, including the Fourth Amendment forbidding unreasonable searches; the First, protecting individual thought and the right to associate privately; the Third, forbidding housing troops in your house; the Fifth, providing that you may not be forced to testify against yourself; and the Ninth, which says that the enumeration of specific rights in the Constitution won't take away the others that aren't listed.[79] The Court held that those provisions imply a right to privacy, at least for very personal decisions such as reproductive choices between married people.[80]

The Court in later cases held that privacy is protected in the concept of due process and liberty guaranteed to all by the Fourteenth Amendment.[81] This amendment, which we mentioned above, states, in part: "nor shall any State deprive any person of life, liberty, or property, without due process of law. . . ."[82] The privacy right arising from this clause prohibits governments from imposing undue burdens on those who would seek abortions of a fetus before it's viable,[83] from interfering with decisions regarding marriage, family

and education,[84] and from outlawing certain kinds of consensual sex between adults.[85] (Current cases concerning sexuality and marriage may be decided on the Equal Protection Clause of the Fourteenth Amendment, which says a state may not "deny to any person within its jurisdiction the equal protection of the laws."[86]) Additionally, the Court has recognized that there may be a narrow constitutional right to privacy in information, which it discussed in cases about certain intimate medical information, former President Nixon's personal papers, and federal contract employees' privacy.[87]

State constitutional right to privacy

Whether the Constitution of the State of Connecticut contains a substantive privacy right that's distinct from its federal counterpart is unclear.[88] That said, if the state courts decide that there is such a right, they have the freedom to define that right as broader than the federal constitutional right to privacy.[89]

Brandeis's and Warren's tort, invasion of privacy

Although some states have adopted statutes establishing private claims about privacy based on the tort theories developed originally by Brandeis and Warren,[90] Connecticut does not have such a statute. In Connecticut, privacy claims are based on judge-made law. Although the state's lower courts first considered invasion-of-privacy claims at least as far back as 1959,[91] its highest court didn't officially adopt the cause of action until 1982.[92] In the intervening years, invasion of privacy had split into four separate torts, in large part because the work of William Prosser, who wrote a definitive treatise on torts and directed the *Restatement (Second) of Torts*.[93] Indeed, that *Restatement* is so influential that the Connecticut Supreme Court adopted its formulation of the four:

> (a) unreasonable intrusion upon the seclusion of another;
>
> (b) appropriation of the other's name or likeness;
>
> (c) unreasonable publicity given to the other's private life; [and]
>
> (d) publicity that unreasonably places the other in a false light before the public.[94]

Unreasonable intrusion on the seclusion of another

The first tort on the list, unreasonable intrusion on the seclusion of another, requires that a plaintiff show both an invasion of his or her privacy and that it would offend a reasonable person.[95] In other words, it's not enough that the plaintiff was actually offended; the plaintiff must show that a person of "ordinary sensibilities" would be, too.[96] The *Restatement* explains that such an invasion may be in a home, hotel, or another other place where one reasonably expects privacy.[97] The intrusion might be physical or with the aid of a listening device, binoculars, or a camera.[98] As it happens, an actionable invasion with binoculars or a camera might even happen in public, for there are things that can remain private even while you're in public—such as your underpants (the *Restatement's* example).[99]

Applying these rules, Connecticut courts have permitted a few claims to proceed. For example, one court allowed a woman to try a claim that the defendant badgered her at home and in a hospital bed over her husband's debt.[100] Another let a woman press a claim for unreasonable intrusion against a salesman who entered her hospital room, posed as a medical person and ineptly treated and injured her.[101] Other courts have allowed claims under this tort for sexual harassment involving unwanted touching and—even without touching—comments of an intrusive and offensive nature.[102]

Those who have been unsuccessful with this tort include a rental car driver who failed to present the Connecticut Appellate Court with any legal authority that he may expect privacy on the roads.[103] The court consequently affirmed the jury's finding that the car rental company hadn't invaded the driver's privacy by tracking his rental car with GPS and automatically deducting money from his bank for speeding (although he did win a claim under the Connecticut Unfair Trade Practices Act).[104] Similarly, another court held that private investigators' long-term video surveillance of a woman pressing a worker's compensation claim was not actionable because it was done reasonably and in public places, and a federal court held that no state common-law expectation of privacy warranted sealing videotapes of women walking into an abortion clinic from a public street.[105] Some decisions in these cases are limited to specific circumstances,

such as when a man sued his boss for listening to his calls but lost because the workplace required an open door and because he actually knew that his secretary was eavesdropping and reporting to his boss (although he won on a state-law wiretap claim).[106]

Other plaintiffs have lost because the intrusion wasn't objectively offensive. To this end, one Connecticut court rejected a claim that hospice workers had interfered with his family life by asking him to leave his daughter's room, failing to tell him that she signed a letter asking for cremation against his religious beliefs, and keeping him from her other family members after her death.[107] Another held that merely videotaping a property without revealing any personal details of the owners' lives wouldn't offend a reasonable person.[108]

All that said, even where there's an objectively offensive invasion, a successful plaintiff must prove that it was intentional.[109] One plaintiff lost a claim that his neighbor let a dog into his house—which might offend a reasonable person—because there was no evidence he did it on purpose.[110]

Appropriation of another's name or likeness

The second invasion of privacy tort in Connecticut is appropriation of another's likeness or name, sometimes called the right to publicity. When the defendant takes the plaintiff's image or name and, without permission, uses it for his or her benefit, the plaintiff may have a remedy under this tort.[111] As the *Restatement* explains, the appropriation usually must be for some commercial benefit such as an advertisement; while it may be for some other benefit, it's not enough to show simply that your picture was printed in a periodical or else there'd be no end to liability for newspapers and magazines who print pictures of people on the street.[112]

The first reported case allowing an invasion of privacy claim in Connecticut was for one of appropriation. There, a girl's mother brought a claim on her daughter's behalf against defendants who'd used the girl's picture in an ad without her permission.[113] She was allowed to go to trial where she'd have to prove that using the picture would be offensive to a reasonable person.[114] In another case, a plaintiff sued and won a privacy claim because the defendants had

used his name to press a suit that had nothing to do with him yet which subjected him to public ridicule.[115]

Unreasonable publicity of private facts

The third privacy tort, unreasonable publicity of private facts, requires the plaintiff to show that someone has broadcast private facts that were of no legitimate public concern, and that he did so in a way that would offend a reasonable person.[116] Whether there's a public benefit to knowing the facts is a consideration, as is how deeply into your private life the publisher dug, and whether you yourself are to blame for making yourself notorious.[117]

To publicize the claim means telling more than just a few people, and it cannot include republishing facts that have already been published. Moreover, facts adduced at trials, criminal or civil, generally cannot be the basis for a tort claim.[118]

But even if the publicity element is met, many claims fail because there's a legitimate public interest in publishing the facts. In 1982 when the state's highest court adopted this tort, the plaintiff developer who had sued a newspaper for publishing an account of his mall as a badly located "sore spot," "ghost-town," and a "mere shell of a shopping center" behind whose "pretty exterior" lay numerous problems lost because the development was a matter of legitimate public interest.[119] Similarly a woman lost a claim over a "lurid" newspaper account of her life because the story involved a man's disappearance, a matter of public concern.[120] And a news story about a man who was involved in heroin smuggling was a matter of legitimate public interest, and no basis for a privacy claim.[121]

And, as we've said, the defendant's action must be the kind that would offend a reasonable person. That's supposed to be an objective standard.[122]

Publicity that unreasonably places another in a false light

The final privacy tort, publicity that unreasonably places another in a false light, involves publication of a false statement that the defendant actually knew to be false or that she published recklessly.[123] For the claim to succeed, the falsehood must be offensive to a reasonable person, and not just a hypersensitive plaintiff.[124]

Defamation and false light claims are similar and may be based on the same facts, such as when a woman sued based on an article suggesting that she'd lied to prevent her roommate from being implicated in a robbery.[125] But, unlike defamation, false lights requires publicity, which means more than telling just a few people.[126] Consequently telling a dozen people about plagiarism accusations against a professor wasn't enough to publicize it.[127] Likewise lying to employees about a fellow's misconduct doesn't amount to publicity[128] while announcing it to the press might.[129] That aside, there are instances when the law requires reporting, such as when a law required a nuclear power company to report an employee who drank to the federal government, so there could be no suit.[130] And certain statements are privileged from suit, such as most employers' references[131] and statements made in court.[132]

Even when the publicity element is met, truth is an absolute defense.[133] A simple mistake is not enough—as when a paper printed that a woman had died in a car wreck.[134] And sometimes the statement may be purely one of opinion.[135]

One court fudged the difference between opinion and fact to permit a sympathetic plaintiff to recover.[136] That case arose when disc jockeys at a Hartford radio station played a mean-spirited game called "Berate the Brides" asking listeners to look at wedding announcements in *The Hartford Courant* and pick the ugliest bride for "dog of the week."[137] When a woman whom they victimized sued, the court held that it was well known that brides make themselves look their best for their weddings and that the comments were therefore factually false for purposes of the claim (although that conclusion might not be strictly correct).[138]

Finally, when all these elements are met, the publicity must still be objectively offensive. To this end, a marketing director of a company that made pet-health products was permitted to recover when his company falsely attributed his name to a letter criticizing the Food and Drug Administration.[139] False accusations of extortion against a blogger also met the standard.[140] In contrast a newspaper story about a visitation battle between parents and grandparents that falsely stated that the grandparents hadn't seen the child in a year didn't.[141]

While these tort cases all implicate privacy rights of a kind, most of them are not the kind of rights that the ACLU of Connecticut typically advances. That's because the ACLU of Connecticut's mission is to protect our civil liberties from government abuse by advancing the Bill of Rights and the Constitution of the State of Connecticut.[142] To be sure, the division between common-law privacy-tort claims brought against individuals and companies and constitutional-tort claims brought against government employees isn't perfectly clear-cut. After all, a tort case for invasion of privacy may be brought against a state employee under certain circumstances (there's a thicket of law concerning governmental immunity that we needn't explore).[143]

That said, common-law privacy suits—when pressed against newspapers and in other instances—might actually conflict with other constitutional rights, such as speech, putting the ACLU on the other side of the matter. That's just what happened in the recent case of *Snyder v. Phelps*, in which a religious figure and his family and congregation went around picketing military funerals with hateful signs such as "Thank God for Dead Soldiers," claiming that the death of each soldier was divine retribution for the military's perceived support for gays.[144] The family of the deceased pressed a claim for invasion of privacy (under another state's law).[145] But if the court had awarded damages or ordered the preacher and his family to stop the picketing, the effect would have been to stifle their rights to speak freely under the First Amendment to the Constitution of the United States.[146] The National ACLU, with which we're affiliated, argued against the dead soldier's family's privacy claim and agreed with the result that the First Amendment trumps tort law.[147] And, while we stridently disagree with Phelps's and his family's and congregation's hateful anti-gay message, we support their right to express it.

Statutes

As mentioned above, many of the most important privacy laws are statutes enacted to address particular topics. Examples are federal wiretapping laws that provide greater protection than the Constitution by spelling out exactly when the government may tap your phone, and penalize private individuals who do so unless

someone on the line has given permission,[148] or the Connecticut wiretapping laws that, unlike federal laws, don't permit bugging and do include a right to sue when a call is recorded unless everyone on the line has consented.[149] Statutes like these may curb governmental behavior as constitutional provisions do and individuals' and companies' behavior as torts do. Even so, scholars of privacy law very often criticize the current statutory scheme as anything but comprehensive. Instead, it's lamented as an issue-by-issue collection of laws that haven't been thought out and don't address many of the most important issues.[150] For this reason, we intend to address as many of the federal and state issues facing residents of Connecticut as we can, so that this guide might assist lawmakers as well as individuals.

We will occasionally have to address the differences, and interplay, between federal and state statutes. This can become quite complicated. For example, where there are federal and state statutes on point, there might be instances where the federal law trumps, or preempts the state law.[151] But there are still other instances where the state law may provide greater protection than the federal law, just as the state Constitution may do. (That's just in state court, though, because the state can't tell federal authorities what to do.) Last, there are areas where the state—which has plenary powers—may act when the federal government—which has power to enact statutes only for certain enumerated powers—may not.[152]

Contracts

Additionally, there's contract law, which is becoming increasingly important to privacy. After all, when you sign onto a website and use its services, you may be agreeing to a privacy policy. And, with increased surveillance at work, you're more and more likely to be asked to agree to a policy that will cede your expectations of privacy. Indeed, many of these contracts include clauses that waive your right to appear before a Connecticut court or to have your dispute settled under Connecticut law.[153] Much of this contract law is regulated as we'll see in the sections on *Privacy at Work* and *Privacy in Our Information*. But, because it has long been known that nobody reads the kinds of form contracts you enter into online,[154] and that you

might feel obligated to agree to terms at work, we believe that there may be instances where greater regulation is required.

Court orders

Finally, there's one last general principle that we should introduce here, which is that almost anything that you reduce to writing, any trail you leave at work and online, and the substance of almost any conversation—among other things—might come to light in a civil lawsuit. That's because both the Federal Rules of Civil Procedure and the Connecticut Practice Book say that anything reasonably likely to lead to information relevant to the suit is subject to discovery.[155] The only exception is for privileged information[156]—that is, correspondence or conversations with your lawyer for the purpose of acquiring legal advice, covered by the attorney-client privilege, or certain other conversations or correspondence with your spouse or a psychiatrist, for example.[157] With some exceptions, a court may not force you to divulge those.[158]

To be clear, if a document is subject to discovery, it might ultimately be filed with the court and then anyone can see it.[159] So may transcripts of your testimony about private conversations. And there's the additional point that, even if a document isn't filed, it might leak to the public. The court has the discretion, in limited circumstances, to enter a protective order to keep that from happening.[160] Also, there are some instances when you may file a suit anonymously, if there's a stigma or risk of harm—as in certain medical cases—and records may be sealed in the rare instance when there's an overriding interest.[161]

Criminal proceedings, too, are very public affairs—although they're subject to different rules than civil proceedings. And they remain so long after the fact. Connecticut law renders public records of convictions and even police reports, unless they contain information that would interfere with the police doing their job or might reveal information about juveniles and sexual assault victims.[162] That said, if you're charged but not convicted, the records are erased after the case becomes final, so too when the conviction is expunged.[163] Even so, news and other accounts of a charge or conviction might remain online.

WATCHING US WHEREVER WE GO

In 1890, Brandeis and Warren were most concerned about advances in photography that would permit print journalists to expose anyone in an embarrassing moment.[164] Over one hundred twenty-two years later, new advances in photography still pose some of the biggest challenges to privacy law. That's because there's no longer any need for a photographer—automated cameras watch us constantly from shops, street lamps, or police cruisers.[165]

And these ever-vigilant cameras do far more than just prevent shoplifting or ticket people illegally passing a stopped school bus.[166] They enable police to record every license plate they encounter for ever-growing databases.[167] With the help of facial-recognition software, they will be able to track your movements across a city.[168] And, soon enough, limits will erode even further because the Federal Aviation Administration is in the process of licensing camera-fitted unmanned aircraft—or drones—for law enforcement.[169] They will certainly supplement and might even replace fixed cameras.

But that's not the end. There are plenty of other ways our movements are being tracked. For example, GPS technology in our cell phones enables software applications but also tells service providers where we are.[170] (And even older cell phones track users through signals to the towers.[171]) Likewise, computers in our cars use GPS to catch thieves or facilitate rescue after accidents while giving up our location.[172] Moreover, we let everyone know where we go when we use an E-ZPass to pay tolls without having to fumble for change.[173] And we also give up our location in ways that we might never have imagined, such as by joining Facebook, potentially becoming part of the world's largest database of faces for the facial recognition software mentioned above, or by using mobile devices that are tracked by cookies or through applications whose functions we might not fully understand.[174]

Through all of this technology, movements may be forever recorded such that an entire picture of everyone's private life will emerge: wherever you've gone and with whomever you've been and whatever things you like to do. And, despite the huge potential loss of privacy from the indefinite storage of all this data, there's not

much law to protect us from its misuse. That's because, generally speaking, there are no laws to make it illegal to photograph someone in a public place—indeed, there's a First Amendment right to record or videotape public officials performing their duties.[175] (Of course that right is for persons and not government, and there are some circumstances in which police videotaping protests might chill people's First Amendment rights and consequently be illegal.[176])

In fact, under the constitutional and tort laws, courts have seldom recognized an expectation of privacy in public places, or when you otherwise voluntarily reveal information to the public. Police may walk by your house and look at what's exposed to public view or even fly over your yard without conducting a search and triggering constitutional protections.[177] And, similarly, there's generally no claim under Connecticut's tort law for invading privacy on the street. That's why courts denied invasion of privacy claims by the woman who was taped in public and the car renter who got automatic tickets from a GPS system.[178]

All that said, we believe that constitutional law will soon change in one key respect. For with the new technology that permits police constantly to watch and record you—which they couldn't practically do before—five of nine justices of the Supreme Court of the United States have suggested that they are open to a new interpretation of our expectation of privacy.[179] For, while it's not reasonable to expect that no one can see or photograph you using a public street, you don't expect the police to target and follow you for weeks without its being a search.

Meanwhile, as we continue to press and wait for such a ruling, we'll advocate for statutes to limit how long information may be kept from cameras, drones, license plate scanners, and GPS systems, and also for it to be rendered anonymous wherever possible. To be sure, such statutes will be necessary even if the Supreme Court adopts the hoped-for new understanding of the expectation of privacy. That's because statutes—like state constitutions—may provide additional protections to what's in the Fourth Amendment.[180] Moreover, unlike the federal and state constitutions, statutes can protect us from such non-government actors as criminals and companies that might post the information that they collect on our whereabouts on the internet.

Cameras

Different actors use cameras in different ways to monitor us. First, there's the security monitoring that follows you in stores and coffee shops, and the cell phones that people use every day to snap photographs.[181] Then there are the increasingly present municipal cameras that follow you outside, and which are on the rise in Connecticut.[182] Some of these are already so sophisticated that they can zoom in on and read your papers from a distance, and new technologies are being developed all the time, such as one to record your fingerprints without your knowledge.[183]

The first sort of cameras, which are privately owned and operated, aren't covered by the Constitution at all. There's no statute barring them if they're trained on public places and used in the ordinary course of business—that is, as you'd expect security cameras to be used. There is, however, a Connecticut anti-voyeurism law that criminalizes videotaping or otherwise photographing anyone who is not in "plain view," without his "knowledge and consent" and when there's a reasonable expectation of privacy—at least when it's done with malice or lewd intent.[184] So the coffee shop's owner may have a camera in the dining area or the kitchen but may not secretly film you in the bathroom. (That said, the law expressly forbids videotaping or spying on you in a dressing room,[185] but, oddly, doesn't expressly forbid cameras in public restrooms—although there are provisions protecting employees from bathroom surveillance, as we'll see in *Privacy at Work*.) The same goes for the private cameras that individuals carry about with them everywhere on cell phones or computers. If you're in public, their users may photograph you freely, yet they may not take a picture of you when you're in a private place without your consent.[186] And you should be mindful that there's the possibility that these cameras can be hacked, so that your own computer's webcam or the camera on the computer being used by your neighbor at the coffee shop might be hijacked and used against you. That hacking is illegal,[187] and the picture-taking might be, too, if you're photographed in private. There may even be cases where this or other behavior warrants the application of the state's anti-stalking laws, which criminalize repeatedly monitoring

or following you about in a way that would reasonably cause you to fear for your safety, or another's, or for your business reputation.[188]

Criminal law aside, there are also protections in the common law of torts because, as we mentioned above, it may intrude on someone's seclusion to be photographed in a private place. Indeed it may be an intrusion to photograph a person even in a public place, if you take a picture up somebody's skirt, for example. After all, the *Restatement (Second) of Torts*, relied on so heavily by the state's courts, explains that even in public there are things that remain private, such as your underpants.[189] (Still, photographing someone's underpants in public might not be a crime.[190]) Keep in mind, however, that tort laws permit a person harmed by another's misbehavior to recover money in exchange for the harm (and sometimes to punish it), and unlike criminal laws, couldn't result in the offender being imprisoned.

As for the other sort of cameras, the municipal kind, they fall under a different set of rules. There's no statute prohibiting the use of these cameras in a public place. Nor does visual surveillance from public places constitute a search under the Fourth Amendment to the Constitution of the United States, or Connecticut's Article 1, Section 7—at least, that is, without enhancing technology to see things that no one else can see.[191] To be sure, the police may watch you with regular cameras with ordinary zooms, and they may even fly over your property and your house with airplanes or helicopters, provided that they stay in legal airspace licensed by the FAA and don't peer too much into the curtilage, that area immediately surrounding your house.[192] That's because anybody else could do the same thing—at least anybody else who could afford an airplane or a helicopter. By contrast, monitoring in private places, such as your apartment or house is a search under the Fourth Amendment and Connecticut's provision, so police must obtain a warrant, which may issue only under narrow circumstances.[193] Likewise, authorities must obtain a warrant before using such enhanced techniques as thermal imaging to see things in a dwelling that they couldn't see with the naked eye unless they went inside.[194] (The Court did not decide in *Florida v. Jardines* whether a dog sniffing your door for a whiff of what's inside constitutes such an enhancement.[195])

Still, the distinction between photographing you in a private or public place is in some sense illusory, for you retain some expectation of privacy even in public view. Fortunately, the Supreme Court of the United States has recognized this, albeit obliquely. In holding that the police may watch you from public vantage points with limited enhancements, it has suggested that it might hold that enhancements to zoom in on you and see intimate things about your person, effects or papers would transform surveillance into a search.[196] To this end, the Court explained that watching you by satellite or with telescopic cameras that could zoom in on the tiniest of details "such as a class ring" or read secret papers might be deemed searches.[197] To be sure, the Court was writing in a case that involved surveillance of a privately owned commercial lot rather than of a person on a public street but, by the logic of *Katz*, where you are makes no difference. We consequently believe that some government cameras, such as those that can zoom in on and read private papers or mobile devices that you reasonably think no one else can read,[198] cross that same line.

Drones

While it's reasonable enough to say that only limited enhancements may be used before transforming surveillance into a search, it's difficult to know how this rule will be applied to new technology now unfolding. Here we have particularly in mind unmanned aerial vehicles, or drones. These are the kinds of aircraft that the military has deployed in Iraq and Afghanistan and the CIA in Pakistan, Somalia, and Yemen over the past decade to watch militants and, in some cases, kill them.[199] Now, the unarmed variety is being licensed by the FAA for law enforcement, even at the local level. (The FAA is not going to be issuing commercial licenses until 2015.[200]) So your local police force might soon be deploying its own drones to track the residents of your town, a prospect that's causing a great deal of public anxiety.[201]

But will the Supreme Court hold that surveillance with these vehicles is no different than helicopters flying over your house, or watching people with limited enhancements in the streets? There are no court rulings yet, but there are certain salient differences between police helicopters using limited enhancements and these

drones. First, we expect that these vehicles will have extraordinary telephotographic technology. If so, the use of those cameras to zoom in on intimate details nobody else could see would be a search, requiring a warrant. Second, and just as importantly, they're small and cheap and may be operated around the clock, unlike helicopters.[202] So they will eliminate the practical limits on how long police may watch your property from the skies, in the same way that fixed surveillance cameras removed the practical limits on stakeouts.

The International Association of Chiefs of Police has published guidelines to limit the use of drones, contemplating warrants and destruction of images collected.[203] But we don't think these guidelines are enough, and whether police will actually follow them is hard to say. It might just be too tempting to use or abuse drones even without any reason.

Facial recognition software

Several new technologies permit tracking individuals over large areas with cameras that have already been deployed—that is, without dispatching a drone. For example, municipalities will soon have access to facial recognition software that will permit the tracking of a single individual across an entire city and logging of his or her whereabouts, all with the press of a button and a system already in place.[204] What's more, these cities may have ready databases of pictures supplied by the FBI and possibly even unwitting users of Facebook or some other social medium.[205] Facebook already has the technology to link hundreds of millions of names and pictures together in a database.

ALPRs – automatic license plate recognition systems

Police in Connecticut have affixed cameras to their cruisers to scan for license plate numbers and have, since at least 2009, been collecting the plate numbers and locations of cars they encounter.[206] At least ten municipalities have pooled together all the data that they have collected, which reveal precisely where each car was and the exact time it was scanned. Another fifteen municipalities are planning to do the same.[207]

These camera systems are called automatic license plate recognition systems. They're legally restricted in some states, including New Hampshire[208]—but not Connecticut. Collecting data on drivers might legitimately benefit the public through better enforcement of traffic and parking laws, finding stolen cars, and in tracking the cars of dangerous criminals. But the data is being collected on all cars, regardless of whether there's reason to think the drivers did anything wrong. And the indefinite storage of data on wherever everyone passing through Connecticut has driven creates tremendous potential for abuse. Aggregation of this data over years means that police will be able to keep tabs on everyone indefinitely.

The potential abuse of such data by police is alarming; even more so is the prospect of it ending up in the hands of some private actors, such as stalkers. After all, there's nothing to keep someone from filing a Freedom of Information Act request for the database, which we have already done.[209] Consequently, the ACLU of Connecticut is supporting a bill to limit the amount of time that the police may keep this information, limiting the potential for abuses.

GPS and cell towers

Tracking by GPS and cell towers might soon force the Supreme Court to reexamine whether the time dimension of constant surveillance will constitute an enhancement that—like the satellite that can zoom in on the smallest item—transforms merely watching someone into a search. If you carry a cell phone, the service provider may learn where you are whenever the phone is switched on.[210] That's because the phone sends the service provider a signal whenever you use it. This happens through the cell towers themselves, which show what phones have accessed them and which may even triangulate the phone's location.[211] And it happens through GPS services for directions and local weather.[212] Also, it's possible for the company to track, or "ping," a cell phone equipped with GPS by sending a signal that its user won't detect, and which will show its current location.[213] Software companies often do something similar with smart phones or laptops by sending cookies for numerous marketing applications that track consumers.[214] And, as we've already said, other ways of tracking you through GPS include the computer in your car for navigation, anti-theft, or emergency accident notification services.

Your contract with the service provider governs how you consent for the data to be used, but those kinds of contracts are a take-it-or-leave it proposition. What's worse, it has long been known by contract scholars that nobody reads form contracts like those your providers use, and people may be even less likely to read terms in contracts made by using a website or clicking that they agree to certain terms.[215] So you may have no idea what the privacy policy says. Nonetheless, there's some relief because consumer privacy policies on the internet are regulated by the Federal Trade Commission, whose job it is to uncover deceptive and unfair practices and hold companies to their promises of privacy. (We'll discuss that more in the section on *Privacy in Your Information*.) And federal and state statutes may make it illegal for private individuals and companies to hack electronic communications including location data.[216] These statutes also prohibit your provider from releasing electronic communications or from releasing or selling location data without your consent and create both criminal and civil penalties for those who violate them.[217]

Currently, no federal statute expressly regulates law enforcement's use of GPS.[218] Lower courts have split over the extent to which the Stored Communications Act (part of the Electronic Communications Privacy Act) together with the PEN Register Act permit law enforcement to access cell-phone location data.[219] (The ACLU's position is that warrants are required, especially for long-term and very precise short-term or real time tracking.) But, where it does apply, the Stored Communications Act allows police to obtain certain cell-phone location records with a court order issued on a showing of "specific and articulable facts" to demonstrate that the records are "relevant and material to an ongoing criminal investigation"[220] —a lower standard than the probable cause needed for a warrant. Moreover, the statute allows providers voluntarily to turn location records over to government authorities when there are certain exigent circumstances.[221] (An analogous Connecticut statute lets police access cell phone and internet subscribers' records with "reasonable and articulable suspicion" and requires notice,[222] although police apparently believe they may sidestep it and use the voluntary disclosure provisions of federal law.[223]) And police

haven't been shy about asking for these records. An investigation by Congressman Edward Markey of Massachusetts revealed that providers have responded to 1.3 million requests by law enforcement, some of which were for location data.[224] (This reported number isn't all requests or court orders, because providers say that they received some warrants, too.[225]) At least as far as long-term surveillance is concerned, we're confident that these warrantless standards won't last.

As it now stands, some federal appellate courts believe that precedent by the Supreme Court of the United States says that using GPS to track somebody in public places isn't a search.[226] That's because of *United States v. Knotts*, a case involving government agents putting a beeper in a barrel with the owner's permission and then giving the barrel to the dealer who transported the barrel unawares, all the while being tracked.[227] In *Knotts*, this tracking was held not to be a search because the beeper simply allowed the authorities to follow Knotts on the public streets, where anybody could have seen or followed him anyway.[228] Even under this reasoning, the result would be different if the tracking invaded a home, which is what happened in *Karo*, another beeper case.[229] Consequently, using the beeper in the latter case constituted a search.[230]

Still, one federal appellate court held that the holding in *Knotts* didn't control when the tracking went on for four weeks. In *United States v. Maynard*, the United States Court of Appeals for the District of Columbia held that such long-term surveillance with GPS crossed the line and became a search (a possibility that the *Knotts* Court itself left open).[231] Several trial courts—including one sitting in the Second Circuit, the geographic division of the federal appellate court system where Connecticut lies[232]—have agreed. But the U.S. Court of Appeals for the Second Circuit itself, whose opinion would be binding on all lower federal courts in Connecticut, has not ruled. And, when *Maynard* went up to the Supreme Court, the Court affirmed it on very different grounds.

Maynard reached the Supreme Court under the name *United States v. Jones*. As the Court explained the facts, the authorities were watching Jones and got a warrant to track him on the roads with GPS.[233] The problem was that they put the credit-card sized

tracker on his wife's car—which she let him use—outside both the time and geographical limits placed on their authority, so they were effectively acting without a warrant when they followed him for 28 days before arresting him.[234]

The Justices all agreed that this conduct was a search, but split about why. A five-to-four majority held that there was no need to determine whether using GPS to track someone over a long time violated the two-prong expectation of privacy test because placing the tracker on the car without Jones's permission was a trespass, and consequently a search.[235] (There was no similar problem of trespass in *Knotts* or *Karo* because the defendants in both cases came into possession of containers with the beepers already inside.[236]) But four Justices—led by Justice Samuel Alito, who's usually aligned with the conservatives on the Court—weren't convinced.[237]

In his concurring opinion, Alito expressed doubt about the viability of the trespass test, favoring the two-prong expectation of privacy inquiry.[238] Among other things, he explained that it wasn't even clear under common-law principles that placing the credit-card-sized tracker on the car was actionable because it was so small.[239] And, anyway, the property-law analysis was unhelpful, in part because it was Jones's wife's car and not his own and that might demand different results in different states.[240]

More to the point, Alito believed that the Court was punting the real question: does long-term use of GPS to track a vehicle violate a reasonable expectation of privacy?[241] Surely the police couldn't really have physically followed Jones around for weeks without a huge team and a great deal of expense.[242] And that's a problem, because the rationale for the distinction between a search and mere surveillance has always turned on the idea that they were just doing what anybody can do.[243] So Justice Alito and those who signed on his opinion would have held it a search for that reason.[244] Of course that leaves the problem, as Alito and Scalia (on the other side of the issue) both noted, of exactly when mere surveillance becomes a search.[245] And, to be sure, that might be a big problem. But, Justice Alito wrote, it's better addressed in most cases by the adoption of a statutory scheme to say when police may and may not

use GPS tracking.[246] That worked in wiretaps, after all, for those cases are now decided entirely on statutes without the need to reach constitutional questions.[247]

Of course a concurrence is not the law, and so Justice Alito's opinion might be no more than an objection noted. But, while four Justices can't decide what the law is, a fifth—Justice Sotomayor, who had joined the majority in *Jones*—wrote her own concurrence expressing sympathy for Justice Alito's view.[248] She wrote that the case may soon come when there won't be any physical trespass, no card affixed to the car, and then the Court will have to decide whether use of GPS might constitute a search, even when it's employed for only a short time.[249] She added, for that matter, that the rapid advance of technology may force the Court to revisit and (she hinted) modify the doctrine that says that information that you've already shared with a third party isn't private, noting that people probably don't expect GPS services to be turned against them.[250] (She meant the constitutional third-party doctrine announced by *Miller*, the case that said bank records can't be private because you've already shared them with the bank, now modified by statute.[251])

E-ZPass

Perhaps this third-party doctrine poses problems for privacy in light of radio-frequency identification (or RFID) technology. An RFID device sends a signal to a tracker to permit it to reveal its location and whatever coded information on it. It's used in keyless car entry, increasingly in retail goods and even body implants, and it's also in the device called an E-ZPass that you might keep on your windshield, and which sends an identification code signal over hundreds of feet to notify an automatic toll booth that you've passed through it and will pay the toll.[252] But E-ZPass also leaves a history of where you've been that might be of interest to snooping eyes.[253] These might be police—for there are no federal or state cases stating whether their monitoring of these booths or chips is a search. Or they might be criminals or stalkers, or sophisticated technology-equipped private investigators, who might send cookies to the chip to see where it has been.

Legislation

In our view, the federal and state constitutions will no longer bear continual encroachment through the physical enhancements of surveillance (such as the telephoto or thermal cameras that ordinary people can't use) or in the temporal dimension, when police with tracking technology follow us about wherever we go and as long as they please. But we don't intend to sit around and wait for the courts: instead, we think the time to act prospectively is at hand, and to create a comprehensive statutory scheme that will keep the police from collecting and indefinitely storing information on all of us without any reason to believe that we've done anything wrong. This legislation should be both federal—to govern the FBI and all the other agencies—and state. And it should set the period during which police may individually target and observe us as no longer than they would be able to do without the enhanced technology, preserving the expectation of privacy that we have until now enjoyed.

To make these statutes effective, they must apply to all these means of following us about, including municipal cameras that permit tracking with facial recognition or fingerprint-reading software, license plate scanners, drones, GPS, cell-tower data, and to all other such technologies. They should forbid the private use of license plate scanners, facial recognition software, fingerprinting cameras, or drones—lest they be made available on the internet or used to stalk. And they must limit the instances in which police may use cameras with facial recognition or fingerprinting or other tracking software, license plate scanners, drones, GPS or cell-tower data.

There should be standards for tracking of individuals with any of the technologies possessed by police. Short-term targeted surveillance with enhanced tracking technology such as license-plate scanners must not be conducted unless law enforcement authorities can demonstrate reasonable suspicion that the surveillance will uncover evidence related to an illegal activity. That said, if technology permits authorities to see details others couldn't see or to track or observe someone in real time and precisely (as GPS does) or in a private place like a home, even short-term surveillance requires a warrant or some recognized exception to the warrant requirement. There must

be a warrant for any long-term surveillance or retroactive tracking through enhanced technology, with ongoing judicial supervision. This should be based only on particular facts and probable cause for a specific crime, with limits on when and where the spying may be conducted. Anyone who has been the target of individualized tracking should receive notice and a return of the warrant should be made to explain what police did when they executed it. To the extent the information is collected from license plate scanners or drones or other cameras using facial recognition software, it must be destroyed or rendered anonymous (so that it may be recovered for investigations approved with an appropriate warrant or court order) within a short time, and never permitted to be seen by anyone except the target of the tracking.

Likewise legislation—both state and federal—should limit what information telephone and other companies may collect on our location and how long they may keep it, and should ensure that the information is not shared except by terms made expressly clear to anyone using the service nor turned over to police without probable cause and a warrant following the notice and particularity standards we've just stated. The current scheme—under the Electronic Communications Privacy Act and the Stored Communications Act and its state analog—has proved itself a mess. It doesn't squarely address GPS and its ever-increasing ability to track us so precisely,[254] and has left plenty of room for the abuse uncovered by Representative Markey. A simple warrant scheme for all location data will be better suited to our constitutional rights.

Finally, any evidence seized illegally under this legislation should be suppressed.

It's important to remember that we're talking about limiting only what the police may do without having reasonable suspicion or probable cause. There's no reason to think that constantly watching everyone without any reason to suspect wrongdoing is workable or effective. And, when police have cause to believe that using this technology to target an individual will lead to evidence of a crime, they will be free to do their jobs and to use every technology at their disposal to catch the perpetrator—subject to the warrant requirement or a recognized exception.

Is constant surveillance bad policy?

Ordinary security cameras used in public places will continue to be legal, but the municipalities that increasingly rely on them should consider whether they're good policy.[255] Although there are some anecdotes of catching a criminal before he does harm, including the apprehension of the would-be Times Square bomber in our own state,[256] security cameras aren't always as useful as we are led to believe. Indeed, there are studies to indicate that more cameras don't deter crime[257] and are ineffective at solving it.[258] There's also the problem of relying too much on cameras, which can be expensive, and taking money from where it might be better spent, such as on more police officers.[259] Furthermore, cameras have turned out to be susceptible to abuse, including racial profiling and stalking women.[260] Last, commentators have suggested that cameras—even when they're used properly—will pressure people into conformist behaviors to avoid standing out for the camera.[261]

LISTENING TO WHAT WE SAY

How different talking on the phone has become since *Katz*, the phone booth case. Just think of when you've been in public and felt forced to listen to a loud person on his or her cell phone. Maybe you felt as if *your* privacy was invaded.[262] Indeed, we now talk not just on cell phones but cordless phones or cell phones as walkie talkies, which can easily be overheard. Or maybe we don't talk at all but text or use the internet for email and Twitter and cloud computing and do it at remote locations such as libraries and cafes and over Wi-Fi networks with dubious security. Most of us never even consider how the law protects our privacy while we use these devices, although there's no question that most people do expect *some* privacy on them – even such people as the director of the CIA, who you'd think would be pretty careful.[263]

Constitutional protections against listening to our conversations

It's our experience that on the few occasions when people do think about privacy while using these technologies they assume that the Constitution will protect them. The reality is, however, that constitutional law is not the only privacy protector when it comes to listening to what we say.

As a matter of fact, the federal Constitution was initially held not to apply to wiretaps at all. Back in 1928 when the Supreme Court heard its first wiretapping case, *Olmstead*, it used the only test it had to decide if there was a search: whether there was a trespass.[264] There wasn't. Instead, government authorities had fiddled with the wires outside Roy Olmstead's residence without ever going inside.[265] Justice Brandeis, who had co-written *The Right to Privacy* 38 years earlier, dissented, lamenting the invasion.[266] But his view wasn't law, and the outcome he sought wouldn't be reached until the Court heard *Katz* in 1967.[267] Famously writing that the Fourth Amendment "protects people, not places," the *Katz* Court overruled *Olmstead* to hold that, despite the lack of trespass, there was a Fourth Amendment violation.[268] And Justice Harlan wrote his influential concurrence setting forth the reasonable expectation of privacy test.[269]

As it happens, *Katz* wasn't a wiretapping case because police had listened only to Katz himself and not the line.[270] It was a bugging case.[271] (Notably, some bugging cases would be searches even under *Olmstead* if, for example, police went into a home and planted a microphone.) But the rule is now the same for all kinds of electronic eavesdropping whether it's wiretapping or bugging: if it violates an actual and reasonable expectation of privacy, it's a search.

However easy it is to state that rule, courts have found it anything but easy to apply. It stands to reason that our loud cell phone talker might not have a reasonable expectation of privacy in the things he yelled into a crowd, while the things he said would be protected if he were speaking into the same cell phone quietly and away from the group. But some things that you might think are constitutionally protected aren't. For example, there is no constitutional protection when one of the parties to a conversation consents to having that conversation recorded or overheard, even if the consenting party is a police officer seeking to gather evidence. Indeed, the Court has upheld the conduct of a police informant who went undercover and was invited into a defendant's house wearing a wire.[272] Also, the Supreme Court held in *Smith v. Maryland* that police may use a device called a PEN register to learn what numbers you've dialed from your house, and that's not a search if they don't listen to what you said.[273] That's because of the so-called third-party doctrine of the bank case, *Miller*, mentioned above. (Just as Congress responded to the bank case, *Miller*, it blunted the ruling in *Smith* by enacting the PEN Register Act, discussed below, to govern when police may use these devices.[274]) Likewise, while you have an expectation of privacy in your computer and cell phone and the messages on them,[275] that same third-party doctrine may mean that many things you post on the internet and some that have already been sent by email and received by another person might not be protected.[276] (The ACLU believes that people enjoy a reasonable expectation of privacy in much of their internet use and in emails unless they're meant to be public.) And there are areas that simply haven't been clear, such as whether it's a violation of the Fourth Amendment to listen to a cordless call, which may not be encrypted like a cell phone. That depends on how easy it is for someone to overhear it.[277] (Given new

models, we believe they're protected now, and, as we discuss below, cordless phones are protected by statute also.[278])

Despite this lack of clarity, the good news is that the Court was pretty clear when it comes to the next question: when is a search by electronic eavesdropping reasonable? In *Berger*, decided the same year as *Katz*, the Court set forth these requirements for a wiretapping statute to be constitutional:

1. There must be a warrant issued by "a neutral and detached authority" to determine whether there's probable cause;[279]

2. The applicant for the warrant must say what crime is suspected, where he'd like to search, and whom or what he'd like to seize (or that is, what conversations he'd like to hear);[280]

3. The order has to say when the wiretap will stop;[281]

4. There has to be notice or some reason why it can't be given;[282] and

5. There has to be a return.[283]

The *Berger* Court's analysis applies to all electronic eavesdropping, wiretapping and bugging, too.[284]

NSA data mining

Despite these clear requirements, warrantless searches have been conducted in the name of national security since shortly after the September 11, 2001, terrorist attacks. This spying began under a classified program by the National Security Agency that was kept secret from the public until 2005, when the *New York Times* reported for the first time that the NSA was eavesdropping on thousands of Americans, all without warrants or authorization from Congress.[285]

The program began as an unchecked exercise of presidential power. Relying at first on his legal staff's broad interpretation of executive authority,[286] the president seized on language in a forty-year-old Supreme Court case to justify acting without warrants.[287] As he saw it, the Court in 1972 held that wiretaps and bugging for domestic security threats require warrants but left open whether they're required for foreign threats.[288]

When the NSA-spying program became public, however, the president no longer relied solely on his own branch's inherent authority but invoked also Congress's broad grant of power to use military force in response to the attacks.[289] And this continued until at least 2007, when, the government now says, the original program stopped.[290]

But the monitoring didn't stop, for, while some members of Congress were appalled, others saw a way to approve the program after the fact, and have therefore passed the FISA Amendments Act of 2008 to modify what's called the Foreign Intelligence Surveillance Act (more about that in a bit). Now the current president continues to run a program of NSA data-mining without warrants on the theory that he needs no warrant so long as the target is out of the country, and not a citizen or permanent resident—even if that means listening in on a U.S. citizen on this end of the line.[291]

Even now no one knows for certain what's included in the data collected, though some report that it includes logs of calls dialed or received across the nation and the substance of texts and emails—so much data that there's an NSA warehouse for it somewhere.[292] What's worse, because of the collection's secretive nature, no one knows what controls there are on the data, if any. Still, it's been reported that efforts to render data anonymous and to limit who can see what have both failed, as have efforts to ensure that the program follows even its authors' own broad interpretation of executive power under the Fourth Amendment.[293]

What's worse still, the courts seem unlikely to hear challenges to the program. First, an effort to challenge the original program has hit a snag on the principle of standing—which is the doctrine that says that to bring a challenge in federal court you must have suffered an actual injury—when an appellate court held that, because the plaintiffs couldn't ever know who had been monitored, they couldn't claim that they were injured by the program.[294] And the Supreme Court of the United States reached the same conclusion in a challenge of the 2008 statute by lawyers and human rights activists working for people outside the United States who were possible targets of surveillance.[295]

Influential commentators have pointed out that the dangers targeted by the NSA program include the unimaginable, such as a terrorist attack with a nuclear weapon.[296] Some, including the federal appellate Judge Richard Posner, have argued that the executive is the most qualified to prevent an attack and that involving cumbersome procedures with generalist judges will only get in the way. That's because the whole point is to find out whom to suspect, and, anyway, the minimal (most likely unnoticed) intrusion of mining our communications is little to ask in the balance.[297] But how can we agree that the balance favors the NSA data mining, when we don't know anything about it? The ACLU remains committed to the principles that the judiciary is the final arbiter of the Constitution and that the branches of government ought to check each other with at least some transparency.

Federal statutes concerning electronic eavesdropping

Congress has written a number of federal statutes to prevent eavesdropping by government and private actors alike. We'll start with the PEN Register and Trap and Trace Devices Statute, which isn't strictly an eavesdropping law, and move quickly to the wiretap statute that Justice Alito mentioned in his concurrence in *Jones*, above.

PEN Register and Trap and Trace Devices Statute

The PEN Register and Trap and Trace Devices Statute forbids anyone except a telephone company or a government agent with a court order from installing or using a device to trace communications.[298] Because courts have held that using such a device isn't a search (unless it's used to read numbers dialed after a call is placed) neither a warrant nor probable cause is required.[299] It applies to individuals as well as law enforcement and includes penalties for violations.[300]

The Wiretap Act

The Wiretap Act (sometimes called Title III of the Omnibus Crime Control and Safe Streets Act of 1968),[301] forbids anyone but a designated government official with a warrant from wiretapping you, or bugging oral conversations that you reasonably expect are private.[302] (The law was amended to apply to electronic

communications, too, as we'll discuss below.) As Justice Alito wrote, it's the law that decides most of the law enforcement cases involving eavesdropping. That's because the statute generally provides more protection than the Constitution.[303]

Among other things, it authorizes government eavesdropping only for certain felonies and when there's no other way to get the information, limits who may seek warrants, requires periodic reports to the court, and mandates authorities to minimize what conversations are heard.[304] The target of the tap or bug must be informed of it within 90 days of when a warrant expires, or from when a warrant for listening begun under a claimed warrant exception was denied.[305] And, if government officials illegally eavesdrop on a conversation, they may not introduce it at trial.[306]

As for anyone who's not a law enforcement official with a warrant, the law criminalizes intentionally eavesdropping on calls or private conversations, bans devices that do so, and prohibits intentional disclosure of the contents of an illegally intercepted communication.[307] In addition to creating criminal penalties, the law grants the right to sue someone (not including the federal government) who violates its provisions and, consequently, your privacy.[308] There are multiple exceptions including one to permit people to record their own calls or conversations, or to record them with consent of one party to the conversation.[309] So police informants may record suspects undercover, and employers and businesses may obtain consent to record calls.[310] Notably, there is another exception, based on the First Amendment, for disseminating illegally acquired information if you got it without doing anything wrong yourself.[311]

The Electronic Communications Privacy Act, the Communications Assistance for Law Enforcement Act, and the Stored Communications Act

Originally the Wiretap Act applied only to wires and private oral communications, but it was amended by the Electronic Communications Privacy Act of 1986[312] to forbid interception of email and internet data[313] and wiretaps of cell phones.[314] Additionally, the Stored Communications Act, part of the 1986 law, forbids

accessing communications that are stored on a server, including email and text messages.[315] Again, these communications may be monitored with consent,[316] which might be established in a contract with a service provider.

In 1994, the Communications Assistance for Law Enforcement Act changed the law to forbid eavesdropping on cordless phones, but this amendment came at the price of requiring phone companies to employ technology that facilitates government wiretaps.[317] That said, the amended wiretap law still doesn't apply to signals over open radio waves, which means that it's not clear how well it covers Wi-Fi or other advances in technology that hadn't been thought of at the time.[318] The law also misses silent video surveillance.[319]

Worse still – at least with respect to electronic communications such as email – the law provides far less protection against government snooping than it does against wiretapping or bugging. Indeed, we believe that the statute's provisions fall short of what the Constitution requires. That's because the Stored Communications Act requires warrants and probable cause to read emails and similar communications only when they are 180 days old or less.[320] To access older emails (and, according to the government, unsent drafts or emails that have been opened), the statute says agents need obtain only a subpoena or a court order on a showing of "specific and articulable facts" to demonstrate that the records are "relevant and material to an ongoing criminal investigation," which is a lower standard than the Fourth Amendment requires and which has consequently been held unconstitutional.[321] Such an order is supposed to issue only with prior notice, but notice may be delayed 90 days.[322] Government access to many kinds of customer information and phone and remote computer records likewise comes with a subpoena or court order rather than a warrant, and sometimes without any notice at all.[323] What's more, the providers may voluntarily turn over to the government an inadvertently obtained communication about committing a crime, or any communication in the case of an emergency threatening serious physical injury.[324] Last year alone, providers reported to Congress that they responded to 1.3 million formal and informal requests for caller data and text messages, often complying when the police claimed an emergency.[325]

Still more important, there's no statutory exclusionary rule for electronic communications. If agents obtain text messages or emails contrary to the law, the statute lets the evidence be introduced anyway. That's because the statutory exclusionary rule for illegally obtained communications applies only to wiretaps and bugs.[326] Even so, the exclusionary rule fashioned for constitutional violations might apply.

How well these laws work in reality is another question altogether. Two dramatic recent incidents show their weaknesses. First, the Bush family has recently been the victim of hacking of very personal emails.[327] While there's no doubt that the law forbids this sort of conduct, no one has been held to account. Second, the director of the CIA has been forced to resign over personal emails during a criminal investigation of someone else, which resulted in no charges.[328] In fact, the spillover from the incident appears to have precipitated the resignation of another general caught up in emails that were uncovered during the course of the first investigation.[329] Precisely how those emails were obtained isn't clear, but—unlike the Bush incident—it may be that they were obtained through loopholes, which may mean that there is something wrong with the law's design rather than merely its enforcement.

The Foreign Intelligence Surveillance Act

Let's turn back to spying. Several laws specifically addressing spying on foreign powers and suspected terrorists have amended the Wiretap Act since 1968. When, as we mentioned above, the Supreme Court held in 1972 that warrants are required in cases of domestic threats to national security, it left open the possibility that warrants might not be needed for foreign threats.[330] The president jumped on this opening and began a huge program of eavesdropping.[331] But, after investigation, the Congress perceived that the Executive Branch had abused the loophole, so, in 1978, it enacted the Foreign Intelligence Surveillance Act.[332]

This law required court orders, sometimes called FISA warrants, for wire and radio eavesdropping within the United States.[333] The orders issue from a special court called the Foreign Intelligence Surveillance Court composed of judges from the judicial branch of the

federal government (and there's another special court for reviewing the first court's decisions).[334] If the target of the surveillance is an alien in the United States, the order issues on probable cause that he was a foreign agent, but if the target is a citizen or permanent resident, there must be probable cause to suspect criminal activity.[335] There must also be probable cause that the target will actually use the device monitored, a statement that there was no other way to get the information, and attempts to minimize the intrusion, among other things.[336] Exceptions permit unapproved taps for a short time during war and when the attorney general determines an emergency demands it.[337]

USA-PATRIOT Act

After the September 11, 2001, attacks, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (or USA-PATRIOT Act) and the Intelligence Reform and Terrorism Prevention Act of 2004, two measures that began as temporary laws but have been extended ever since.[338] Together, these laws amended the Foreign Intelligence Surveillance Act to include terrorists as foreign powers, even if the terrorist is acting on his own—a so-called lone wolf.[339] And they currently provide for federal authorities to seek so-called roving wiretaps—which target a person and not a location or particular device—to be supervised by the Foreign Intelligence Surveillance Court and without the notice that would be required under the Wiretap Act.[340] They also permit authorities to issue National Security Letters demanding access to records of all kinds, including travel records, pharmacy records and phone records, all the while forbidding the recipient of the letter from tipping off the subject of the request—although such gag orders have been held unconstitutional.[341]

The FISA Amendments Act of 2008 and Extension of 2012

When it became clear that the NSA data-mining mentioned above exceeded even the USA-PATRIOT Act, Congress amended the Foreign Intelligence Surveillance Act regarding surveillance of aliens outside the United States.[342] The new law requires the attorney general and the director of national intelligence to apply to

the Foreign Intelligence Surveillance Court for an order to conduct surveillance on aliens abroad, without any need for probable cause that the target is a foreign power or its agent.[343] The law doesn't require the government to say what facilities it will target and allows unlimited surveillance for up to a year.[344] While officials may not use the law *intentionally* to target a United States citizen or permanent resident, or anyone in the United States,[345] apparently they may incidentally eavesdrop on such a person without a warrant. And, even though it has been condemned for its relaxation of the standards for obtaining a warrant and the limits it places on judicial supervision,[346] this law has just been renewed for an additional five years.[347]

The extent to which this law is being used to spy on us isn't known. Because the Supreme Court has held that the lawyers currently challenging it have no standing, it might never be known.

Constitution of the State of Connecticut

State law applies as well to wiretapping and eavesdropping, protecting you from government intrusions and from private eavesdropping. Article 1, Section 7 of the Constitution of the State of Connecticut, like the Fourth Amendment to the Constitution of the United States, protects against unreasonable searches and seizures. And, like the Fourth Amendment, it forbids police from eavesdropping without a warrant.

Although the Constitution of the State of Connecticut may provide greater protection than the federal Constitution, at least for those on trial for a state crime (federal crimes tried in federal court are usually governed by federal wiretapping law[348]), state constitutional law generally tracks Justice Harlan's expectation of privacy from *Katz* and the warrant requirements in *Berger*. And it mirrors many other major federal rules, too. So, for example, Connecticut courts reason that, while you have a privacy interest in your cell phone and computer, you might lose your interest in certain information that you've already sent to a third party and which may be obtained from that party.[349] And state courts have also held that there's no protection against being recorded or overheard when you talk to an undercover police informant who has consented to the eavesdropping,[350] as in

the federal informant case. In any event, as under federal law, most eavesdropping cases in Connecticut are covered by statutes (state or federal) without any need for reaching the Constitution.

Connecticut statutes concerning electronic eavesdropping by law enforcement

Connecticut has several statutes governing eavesdropping, but we'll talk first about the one aimed at wiretapping by law enforcement.[351] It's modeled on the federal Wiretap Act but doesn't permit bugging.[352] It applied to cordless phones[353] before they were covered by federal law.[354] It doesn't regulate what officials in other states do, even if someone in Connecticut happens to be on the line.[355] Even so, where the law does apply it's theoretically more restrictive than the federal law.[356] The state law prohibits all wiretaps of the offices of doctors, lawyers, or clergy,[357] says recordings must be sealed and kept confidential, and provides for penalties and for suits for wiretaps that were illegally obtained or disclosed by law enforcement or in violation of the criminal wiretap law, which we'll discuss below.[358] Anyone who's aggrieved by a wiretap obtained illegally under the section may move to suppress it, but the General Assembly in a 2002 anti-terrorism law added a section explaining that a wiretap obtained "in conformity" with federal law may be admitted.[359]

Supplementing the state's wiretap act is a statute analogous to the Stored Communications Act that permits law enforcement officials to obtain a court order on a showing of "reasonable and articulable suspicion" to force any telephone or computer company to turn over basic subscriber data, including names, addresses, phone logs, payment records, and internet addresses as well as all call-identifying information, including when and where a person placed or received a call and to or from whom.[360] Anybody whose information is sought is supposed to get notice within 48 hours after the court order issues, although it may be delayed 90 days where there's a chance notice might endanger someone or result in flight, destruction of evidence, or some other risk to the investigation.[361] Also, the police must report to the chief state's attorney, who in turn reports to the General Assembly how many orders were issued under this section, for what, and what prosecutions resulted from them.[362]

This state statute does not authorize the police to access the contents of a communication.[363]

Fusion Centers

Sometimes, it's not only federal and state laws that work together badly. Sometimes federal and state law enforcement officials have problems interacting, too. At least that was the judgment of both parties in a Senate subcommittee investigating the Department of Homeland Security's so-called Fusion Centers, which have been operating across the country, including in Connecticut, to facilitate information sharing between all levels of government.[364] The theory was that law enforcement had been watching the 9/11 bombers yet failed to recognize that they planned the attack.[365] Better coordination, went the thinking, might prevent future disasters.[366]

Fusion Centers have been a failure. During the more than a year covered by the study, no intelligence produced by the centers led to uncovering a terrorist threat.[367] Many of the reports were frivolous, there were many disturbing incidents of privacy invasions, and there was much wasted money.[368] And the report recommended revisiting whether Congress wanted the program to continue at all.[369]

Connecticut statutes to prohibit eavesdropping by individuals and companies

Criminal laws also apply to eavesdropping in the state. Connecticut makes it a felony to intentionally listen to or record someone else's telephone conversation (including cell phone calls) without the consent of at least one person on the line, or for someone who's not present to use any equipment to intentionally listen to or record a conversation without the consent of at least one person who's participating.[370] (There's an exception for law enforcement officials conducting a wiretap with a warrant.[371]) What's more, it's a misdemeanor to use deceit, threats, or any other tactic to learn the substance of a call from a phone company employee or for such an employee to divulge it without consent.[372] Also, the Connecticut Communications Consumer Privacy Act forbids a person or company providing electronic entertainment services, such as television or cable, from spying on anyone with any equipment that allows it to see or hear what's going on in that person's house.[373]

But eavesdropping isn't just a criminal matter. As we mentioned above, provisions in the chapter on wiretaps by law enforcement permit victims of the criminal wiretap law to sue for illegal interception or disclosure of the communication. A separate state statute creates a cause of action (that is, a right to sue) whenever a private telephone conversation is *recorded* without the consent of *all* parties on the phone.[374] The statute explains that consent must be given, in writing or orally, at the beginning of the recording—but when it's not so expressed, it will be imputed whenever there's a verbal warning at the start of the call or a beep repeating throughout.[375] Of course anyone who has called a customer service line will be familiar with warnings that a "call may be recorded" and the (rather annoying) repeating beep. The statute doesn't apply to eavesdropping by law enforcement, or to various emergencies such as 911 calls, to calls for radio stations to broadcast, to recording someone who's threatening you, or to recording calls that come "repeatedly or at an extremely inconvenient hour."[376] The Connecticut Communications Consumer Privacy Act also has a provision permitting suits.[377]

Hacking

The Electronic Communications Privacy Act and Stored Communications Act protect your emails and other communications but don't necessarily protect all the things you write and keep on your own private computer. State and federal statutes also criminalize unauthorized access of your computer by someone who wants to take information off it or disable it.[378] Because, as we mentioned at the outset, federal law applies only where the Constitution grants it power, the federal law here applies only to certain computers, such as those belonging to banks, the federal government, or those that are used in interstate commerce.[379] There's no such limit on the Connecticut law.

Contracts

You should also be careful before you share the things that you keep on your computer with others, for example the managers of a cloud computing server, to learn who has the right to see it. Contracts are the first source of protection. The same is true of the various web-based companies that make certain privacy commitments through

their privacy policies, enforced by the Section Five of the Federal Trade Commission Act.[380] That said, because sharing with one person means that he or she can share it again, it's better to presume that nothing you send to anyone without a strict confidentiality agreement will stay private for long.

Legislation

Many of these federal and state laws are premised, apparently, on the belief that, because we share emails and texts and other such communications with our service providers—just as we share the numbers we dial with the phone company—we hold only a reduced privacy expectation in them. But that's contrary to how people actually live. Texts have largely replaced talking for many young people, and email is the new way of conducting business, even privileged business with a lawyer. So the idea that these communications deserve less protection than wire communications no longer makes sense.

Consequently, we believe it's time to amend the statutes on the state and federal level to accord all forms of electronic communications the same level of protection that applies to private oral and wire communications. That means that these electronic communications must not be intercepted or obtained by law enforcement officials without a warrant issued by "a neutral and detached authority" to determine whether there's probable cause based on particular facts to justify a belief that particular communications will lead to evidence of a specific crime. It also means that the warrant must specify a certain period of time covered and notify the target (or provide some valid excuse why notice must be withheld), and that there must be a return on the warrant. Moreover, there should be an end to the warrantless acquisition of all our phone logs and records, from which it's as easy to paint a picture of our lives as from our location data. And any communications illegally seized should be suppressed at trial to deter police misconduct.

On the federal level, Congress should end the extraordinary power purportedly conferred by the USA-PATRIOT Act to seize any and all such documents without restriction. It should also mend the gaping hole in warrant requirements left by the FISA Amendments of 2008

for all sorts of communications, including wiretaps. Furthermore, Congress should thoroughly investigate the abuses committed by the NSA, for unlike the proponents of spying, we're unwilling to sanction a program about which we know nothing.

PRIVACY AT WORK

For all the watching and listening we endure in the rest of our lives, for most of us it's nothing compared to surveillance in the workplace. That's because, as we'll see, employees generally have less expectation of privacy at work than elsewhere, which is, in context, pretty scary. But it's also because this kind of monitoring carries the most immediate and likely consequences. If you seem to be violating a company policy, you'll probably be caught and disciplined and might even lose your job.

What's worse is that the issue isn't merely surveillance *in the workplace* for, increasingly, employers monitor their employees outside the office, too. And so they administer drug and psychological tests and watch what we post on Facebook and other websites.[381] Consequently our behavior on our own time and away from work, which used to be a purely private matter, is being treated something like the property of the employer.[382] All that said, some good news is that Connecticut is one of few states that requires written notice of monitoring at work,[383] and it provides other protections, too.

At the outset, it's important to remember that the laws governing government employees and employees of private companies and individuals diverge. Some of the statutes that we'll address apply equally to both, but the federal and state constitutions apply only to government employees. That means that only government employees may invoke the Fourth Amendment when they're being searched, or argue that the First Amendment has something to say about what they may and may not do off duty (although some statutes protecting the right to organize a union, for example, might be relevant for private employees).

Phones

Let's begin with the telephone. The federal wiretap and eavesdropping statutes apply at work but contain an exception for a company that provides telephones and monitors them in the "ordinary course of its business."[384] That doesn't mean listening to personal calls, but, depending on the business, courts have approved 24-hour monitoring of all calls.[385] What's more, there is another exception for listening to calls when a person has consented to be

monitored,[386] and so companies often simply insist that employees consent. That might subject even your personal calls to monitoring, although whether you've actually consented to monitoring of all your calls is decided case by case.[387] A possible scenario is that the company will forbid employees from using work phones for personal calls and listen only as far as necessary to make sure they don't.[388]

Connecticut state laws concerning monitoring at work—which apply to private, state, and municipal employees[389]—are a little more specific. They forbid using any equipment or device intentionally to overhear or record conversations made by an employee about employment negotiations (unless all parties consent).[390] If an employer engages in other telephone monitoring permitted by state and federal law, it must give every employee who might be monitored written notice of what kinds of monitoring it conducts and post that notice where every employee can see it.[391] There's no need for notice under this section if the employer has "reasonable grounds" to believe that an employee is breaking the law, violating property rights, or creating a hostile work environment and if listening would produce evidence.[392] The state's Labor Commissioner may sue on your behalf if there's a violation, though you may not sue under this statute in your own name.[393] Because the notice law is subject to other federal and state laws, if there's someone else on the line who hasn't consented to recording and the call is recorded, that person may sue.[394] And there may be instances when you might press a tort claim or other state wiretap statutes might apply.[395]

These laws aside, the Fourth Amendment may kick in if you're a government employee—Article 1, Section 7, too, if you're a state or municipal employee. The Supreme Court has been very vague indeed about defining an employee's expectation of privacy (noting Connecticut's workplace monitoring statute as evidence of fast-changing attitudes), although you can bet that tapping someone's work phone is a search.[396] The catch is that monitoring an employee at work over a work-issued phone to see if he or she is using it for legitimate employment purposes might be held reasonable, even without a warrant.[397]

Email and other electronic communications

Work email might be even less secure than the telephone. That's because many employers take the view that they own the computers, handheld devices and servers over which email flows, and consequently may monitor anything that passes over them.[398] As with federal laws covering the telephone, there are exceptions in the Electronic Communications Privacy Act to permit interception by employers that operate their own communications systems, and for monitoring in the ordinary course of business.[399] And, as with phone calls, employers may simply require that you consent to monitoring of your emails.[400] For its part, Connecticut law requires an employer to post conspicuous written notice of any monitoring of your office computer (as described above).[401] While public employees might turn to the Fourth Amendment, they won't find any relief if the employer is reviewing emails or texts to make sure they're not using the phone or computer for personal reasons.[402]

Video and other surveillance

Under the Connecticut law governing monitoring of employees, an employer is expressly forbidden from recording, using video cameras, or otherwise electronically spying on you in the places that are established for workers' health and safety, such as locker rooms and bathrooms, but may monitor you elsewhere (as consistent with state and federal law) if it notifies you.[403] This permitted surveillance may include your computer,[404] and lots of employers monitor not only whether you're using Facebook or surfing the web but monitor keystrokes to see how fast people are typing.[405] Again—as with listening to your phone calls—the employer must first conspicuously post clearly worded notice of the surveillance (except in places held out for the public where there are security cameras).[406] And employers may not use electronic surveillance to listen to you talk about negotiating employment contracts or in any way spy on employees organizing a union.[407]

But of course other state and federal laws apply, too, including eavesdropping laws.[408] They don't address the video aspect, only the sound. Moreover, because some eavesdropping is legal with consent,[409] employers might require it. Government employees may

invoke the Fourth Amendment for spying in private places (and some Article 1, Section 7).

GPS

Connecticut employees who drive for a living—such as truckers and even firefighters and police—might be subject to constant GPS monitoring in their work vehicles.[410] It is not clear whether they must be notified under the state's workplace monitoring law.[411]

Testing

Some testing is prohibited for applicants or employees. For example, under both federal and state law, you can't be forced to take a lie-detector test at work or to get a job (although there are exceptions for certain federal employees, state and local police officers, and employees of the Department of Correction).[412] And there are limits to what medical information employers may seek when you apply for a job. That's because of anti-discrimination laws.[413]

Unfortunately, you may be given IQ or psychological tests. And frankly, some of those are most peculiar indeed. In fact, they're downright uncomfortable.[414] While these aptitude and psych-screening tests aren't illegal in themselves, they might be unlawfully discriminatory and therefore barred by state and federal anti-discrimination laws.[415]

Drug testing

Under state law, any potential private employer may ask you to take a drug test, so long as certain procedures are followed, you are informed in writing when you apply, and you get a copy of any positive results.[416] But, once you actually have the job, most private employers may not test you for drugs unless there's a "reasonable suspicion that the employee is under the influence of drugs or alcohol" and that the use "adversely affects or could adversely affect such employee's performance."[417] This provision was enacted, explained the legislature, to provide the same protection for private employees as government employees would get under the Fourth Amendment.[418] Still, suspicionless testing may be imposed if you're in what the Connecticut Department of Labor deems a "high risk or

safety-sensitive" job, if you drive a school bus, if you participate in certain voluntary programs for addiction, or if federal law permits random testing.[419] (This last includes airline personnel, for example.[420]) When a drug test is given, nobody may watch you pee into the cup and any positives must be confirmed with a second test. Results are supposed to be confidential and may not be used against you in a criminal trial.[421] If your employer violates these laws, you may sue.[422] Collective-bargaining agreements can't derogate from the law.[423]

But that's just for private employees. Unlike the monitoring laws above, those state drug-testing laws exclude government employees.[424] Still, government employees may—unlike private employees—rely on the Fourth Amendment or, if they work for the state or a municipality, Article 1, Section 7.[425] Drug tests are searches but, if the job is a dangerous one, they may be conducted at work without warrants and sometimes without suspicion.[426]

Personnel records

Even if you ace all the tests, employers constantly gather information on you during the course of your employment, much of it unflattering, including complaints from coworkers who might have a grudge and be dishonest. Many of us wouldn't like that sort of thing to be shared and will be pleased to learn that there are statutes to prevent its release.

How these files are treated under state law depends whether you're a private or a government employee.[427] Connecticut law divies up private employee records into a few categories.[428] First comes your personnel file, including all the information relating to your job performance and advancement—that sort of thing.[429] It's supposed to be confidential (the same law says your drug-test results are, too), and nothing that could identify you may be released from it without your consent.[430] Still, you may see it and get copies.[431] And you may seek to correct mistakes or at least insert a written objection.[432] The employer must keep the file for at least a year after you've left.[433] Next come your medical files, kept in a separate file, which must also be kept confidential and for three years after you've left.[434] You may request to have your doctor examine those, get

copies, and seek to correct them.[435] Other files for certain kinds of testing will be kept from you if revealing the results will invalidate the test, so will security files detailing the employer's investigation of losses or suspected crimes (but which aren't supposed to determine advancement), and files for grievances and civil litigation.[436] Even though you may not see testing, security, or litigation files, the state's labor commissioner may subpoena them if necessary to adjudicate a complaint.[437]

If you're a state or municipal employee, the rules are different.[438] While there was once a state privacy law forbidding state and municipal employers from disclosing any personal information about employees,[439] that law's been repealed in favor of the state's Freedom of Information Act, which requires disclosure of most government records in the interest of transparent government.[440] That said, FOIA exempts "[p]ersonnel or medical files and similar files the disclosure of which would constitute an invasion of personal privacy."[441] If such records are requested, the employee whose privacy is at issue has a right to object and then the files won't be released until an administrative panel requires it.[442] This language has been interpreted to mean that the scope of the protection is the same as one of the tort claims inspired by Brandeis.[443] But the remedy for aggrieved employees is an administrative procedure set out in code.[444] Your own access to your files, plus an accounting of who else may see them, is provided by the Personal Data Act.[445]

Federal employees may examine records about themselves under the Federal Privacy Act, which provides other protection, too.[446] And, like state employees, federal employees may rely on an exemption in federal FOIA law that says "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy" are exempt from disclosure.[447] Even so, under federal and state law, some personal information might leak out in emails that are subject to FOIA.

Constitutional right to informational privacy

As we discussed above, the Constitution may include a narrow right to informational privacy.[448] So the Constitution *might* provide some protection for government employees from disclosure of

private information, but it's not likely since the right has been held generally narrower than the protection provided in the statutes we just described.[449] This narrow right will be decided by balancing the particular facts of a given case.[450]

Civil litigation and other lawful subpoenas

Despite all these laws, all of your employment records including your personnel file and all the emails and other communications and documents that you created at work might be obtained during the course of related civil litigation. That's because anything that might lead to information relevant to the litigation, and is not privileged, will have to be turned over. Such discovery might include personal information about nonparties, and the court has discretion to enter a protective order to keep it confidential.[451] Intervention by a nonparty to seek (or challenge) a protective order is also possible.[452]

There are also instances, of course, when your employer or someone else might be the subject of a criminal investigation, and that might result in discovery of some of your information. Likewise, national security investigations under the USA-PATRIOT Act might result in the government accessing your work files without your knowledge or consent.[453]

Activities outside the workplace on Facebook and elsewhere

There appears to be an increasing trend of employers watching what their employees are doing outside the office, including monitoring Facebook and other social media to discipline employee conduct that's off the clock and off the premises. And there's not much protection for private employees here. Even so, covered employers may not fire you for a reason forbidden by anti-discrimination and labor laws, and might be forbidden to fire you for organizing or complaining about certain working conditions.[454] Government employees, but only government employees, may claim that the First Amendment right to speech protects their use of social media like Facebook.[455]

Legislation

We believe that the law should more precisely acknowledge the reality that employees incidentally use work email and other

systems for personal reasons, and protections for such uses should be strengthened. The vague standards for privacy that workers can expect should be spelled out by statute on all levels. And in all settings – for private and public employees alike—the legislature should create standards that we can all live with for what workers may say off the job, both in the real world and on Facebook and other social media.

PRIVACY IN OUR INFORMATION

For many years now and to an ever increasing extent, we've all been defined by our information. Since the New Deal, every U.S. citizen and permanent resident has been assigned a Social Security number linked to her birthday and region of birth, and that number has become an all-but universal identifier.[456] With increasing regulations and ever broader information sharing among medical providers and insurers, we've seen medical records given to the government and corporations alike.[457] We're all graded by companies over which we have very little control with credit scores to determine whether we'll get a loan for a car or house.[458] For decades now we've been routinely using credit and discount cards with which our purchases have been tracked and cataloged for sale to other merchants who wish to sell us more.[459] Now these and other identifiers are pooled and all the tracking is done with increasing efficiency over the internet.[460] What's more, our emails are scanned for targeted advertising to our accounts.[461] We increasingly use electronic devices to access our financial records and accounts.[462] Many of us are posting intimate details of our lives on social networking sites to share with ever-growing numbers of "friends."[463] And information tagging has begun in the physical world, too, for companies have started using tiny radio-frequency identification chips to track the movements in their inventory, and our purchases of their products.[464] Such chips might soon be in our driver's licenses, and some doctors have even begun inserting them into patients' bodies.[465]

Of course there are wonderful benefits to much of this technology, and we don't mean to draw a dystopian picture. After all, we've largely benefitted from ways that have made it easier to identify and define ourselves. Some of them, such as the use of a Social Security number, have been (at least partly) successful tools for many decades. Others, such as internet tracking, offer benefits to consumers who want to have information targeted to their desires. And we can hardly doubt the benefits a patient might get from having all of her medical information available to a doctor at the mere scan of an RFID chip.

That said, all these examples, including Social Security numbers, have their downsides, making it easier to counterfeit

people's identity, for example.[466] And more sophisticated means of identifying ourselves—such as RFID chips—might lead to even more sophisticated ways of ripping us off.[467] They might also facilitate ways of tracking us that, as we discussed in the section on *Watching Us Wherever We Go*, might be unwelcome or illegal.[468] Wireless internet access also has opened us up to invasions of privacy, such as the recent shocking example of Google, which has admitted that company employees working on its Street View project downloaded massive amounts of personal data from private wireless networks that they passed.[469]

But perhaps most importantly these technologies are advancing so quickly and being adopted so aggressively that there might be no chance to consider their effects or to make an informed choice about whether to use them. Many of our choices about using a given technology have been made simply because everybody else is using it. Consequently, as many have written, technological advances have gradually diminished the expectation of privacy so that it may soon be such that, at least in some areas of life, we have none at all.[470] That would be a shame indeed, especially if it were done thoughtlessly. And so we must ensure that it is not done thoughtlessly.

Unfortunately, we've discovered in researching information privacy that many of the laws that protect our data were written years before the technology that's now commonplace was developed. While there are a few new and broad-reaching laws, there also is a hodgepodge of various statutes written as issues come to popular attention. The problem is that many things aren't protected and, once information is freely shared, there's no real way consistent with the First Amendment to prevent its further dissemination. So we need to arrive at some method of providing the most comprehensive possible protection for people to ensure that they don't share their data with anybody they don't wish to see it. We're keenly aware that this is an ambitious goal. But the best place to start is to identify as many privacy issues as we can, see how the law covers them, and then propose ways to fill the gaps.

Personal identifying information held by government agencies

When Social Security numbers were first issued, they weren't supposed to be used generally to identify you.[471] But that was a long time ago, and the law doesn't say that anymore.[472] Now, despite confidentiality requirements in the statute, you have to provide your Social Security number whenever you do just about anything with a federal or state government agency, such as filing a tax return or seeking a driver's license.[473] And because the government uses the number as a taxpayer identification, you're forced as a practical matter to give it to such private companies as banks and employers.[474]

The federal Privacy Act of 1974 applies to any individual's personal records held by any government agency "including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."[475] It says that government agencies may not collect more personal information about any individual than they need to, must tell people what private information they hold about them, and mustn't give that personal information out without that person's prior consent.[476] When any government agency asks for information like your Social Security number, the act requires disclosure of whether you need to give it and what it will be used for.[477]

On the state level, there's a law to protect "[p]ersonal data" held by any state agency, which is defined as "any information about a person's education, finances, medical or emotional condition or history, employment or business history, family or personal relationships, reputation or character which because of name, identifying number, mark or description can be readily associated with a particular person."[478] This law, too, forbids agencies from collecting more than they need, requires them to grant access by any individual to her own personal data, and includes certain rules regarding confidentiality, including an accounting of anybody who's seen the data.[479] It doesn't strictly forbid release of personal data—relying instead on these procedural protections and agency regulations for confidentiality.[480] The state's Freedom

of Information Act exempts certain things from disclosure, such as certain privileged and financial records and the names of sex crime victims and information about students, to give a few examples.[481] Also, if you're an employee, certain information like personnel files may not be released under the state's Freedom of Information Act if doing so "would constitute an invasion of personal privacy."[482] Public libraries, which used to be protected solely by an exemption to the Freedom of Information Act, now have a state law requiring personal data to be kept confidential.[483]

Other laws also apply. There are federal and state laws to prevent the state's Department of Motor Vehicles from disseminating data without a driver's consent,[484] although the state law has been criticized for letting the state sell data for some purposes while misleading drivers into believing they've denied consent for all data-sharing.[485] Other specific state laws protect the identity of children given up for adoption and their biological parents, permitting those identities to be revealed in some cases with the appropriate consent after the child grows up.[486]

When government agencies are involved, you may also be protected by the constitutional right to informational privacy, which we've mentioned above.[487] It's surely narrower than the statutes, at least the federal ones, and, in any event, difficult to discern because it requires a delicate, fact-specific balance.[488] Still, it might fill in where there's a gap.[489]

Personal identifying data held by private companies

On the federal level, consumer privacy laws—including subject-specific laws we'll soon discuss, such as Gramm-Leach-Bliley and the Fair Credit Reporting Act—are enforced by the Federal Trade Commission with the help of the newly created Consumer Financial Protection Bureau. Perhaps the most important, and certainly most general, of these laws is Section Five of the Federal Trade Commission Act of 1914, which forbids private individuals and companies from misleading and deceiving consumers.[490] Not strictly a privacy law, the Act prohibits unfair acts and practices, which are those that harm or will likely harm consumers substantially, can't be avoided by consumers, and aren't justified *and* deceptive acts and

practices, where something material is done, said or left unsaid in such a way that's likely to mislead a consumer, and the consumer reasonably misunderstands it.[491] The FTC has applied it to deceptive and misleading promises about consumers' personal information, and against companies that have violated their own online privacy policies (although it's by no means tailored to the internet, which we'll discuss in more detail near the end of this section).[492] The state analog is the Connecticut Unfair Trade Practices Act,[493] enforced by the Connecticut Department of Consumer Affairs.

On the state level there's a 2008 law that more directly protects personal information held by private institutions.[494] It applies to all private individuals and companies subject to Connecticut's jurisdiction who maintain "information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number. . . ."[495] These private data collectors must "safeguard" your information from third parties and may not publish your Social Security number or require you to enter it on the internet.[496] The law carries civil penalties and is enforced by the state's commissioner of consumer protection.[497]

Banks and other financial institutions

The Gramm-Leach-Bliley Act is the most important federal law to protect your banking information. It requires financial institutions to create a privacy policy and safeguard personal information from disclosure unless customers, having received a clearly worded explanation of their rights, consent to certain sharing.[498] The catch is that you receive a notice and have to respond to it or else the institution may assume that you've consented—and thus it's your inaction that permits the institution to share your information.[499] Gramm-Leach-Bliley also forbids obtaining bank information by fraud.[500]

The law allows disclosure to law enforcement agencies[501] that are permitted to obtain information under the Right to Financial Privacy Act of 1978.[502] That law was enacted after the Supreme

Court held in *Miller* that bank records aren't protected by the Fourth Amendment. The law provides for notice and the right to challenge certain subpoenas.[503]

Connecticut law, too, guarantees some privacy in banking. A state law requires a customer's authorization for most disclosures by financial institutions, but no permission is needed for disclosures to medical providers and judgment creditors or in the case of a court order.[504] Similarly, banks may share information with certain state agencies, such as the Department of Administrative Services, the Department of Social Services, and the Department of Veterans' Affairs.[505] And customers must receive notice of subpoenas seeking to force a bank to disclose private information, and may then challenge the subpoena in court.[506]

Credit reports

Credit reports are those detailed financial histories of your credit, payment records, and employment information which—like bank records—include loads of private information such as Social Security numbers.[507] Credit reports are generated by three major credit-reporting agencies: Experian, Equifax, and Trans Union.[508] They play a major role in determining whether you'll be able to finance the purchase of a house, get insurance, or sometimes a job.[509]

Credit reports are governed on the federal level by the Fair Credit Reporting Act of 1970,[510] which requires credit reporting companies to take reasonable steps to ensure the reports' accuracy, limits who may get a copy, and mandates that anybody who takes a so-called adverse action against you on account of a credit report must inform you.[511] The law also creates private causes of actions against certain businesses that don't comply[512] and some causes of action that may be brought only by the government.[513] The right to bring some suits was stripped away by the 2003 Fair and Accurate Credit Transactions Act,[514] which also forbids merchants from printing more than a certain amount of your credit card data on a receipt.[515] State law covers much of the same ground.[516]

These laws notwithstanding, credit reports aren't kept very private. Instead, they're available to potential creditors, insurers, and employers, to name just a few.[517] They're even available for

resale.[518] What's worse, credit reports often contain errors, which can be a serious problem. Fortunately, the laws let you demand a copy of your report and seek to correct any errors.[519] The agency has 30 days to look into your claim.[520] If the agency agrees with you, you may request that it circulate the corrections to whom you designate.[521]

Medical records

On the federal level, medical privacy is governed by two main statutes. The first is the Health Insurance Portability and Accountability Act of 1996,[522] which just about everyone calls HIPAA. The second is the Health Information Technology for Economic and Clinical Health Act, which was the part of the 2009 stimulus bill devoted to digitizing medical records.[523] Together these laws and the regulations enforcing them ensure that your medical records are kept private by limiting use to health care or insurance purposes and by minimizing the release of information.[524] They clarify that, with some exceptions, you may not be forced to sign a privacy waiver before getting care.[525] And they grant the right to see and seek to correct any errors in records held by health plans, so-called health-care clearinghouses, pharmacies and medical research centers, as well as records held in connection with electronic billing. You may also find out who else has seen your records and you may limit access to them.[526] If there's a breach in the security of your electronic records, you're meant to be notified.[527] In addition to these federal laws, the Connecticut Insurance Information and Privacy Protection Act requires insurance companies to provide an accounting of what personal data they hold and who has seen it.[528]

These laws don't shield your information from everybody. Employers might be entitled to some health information—though they may not discriminate against you for it.[529] So may certain government agencies, including those that administer Medicare, Social Security Disability and workers' compensation insurance, as well as law enforcement, which may see any pharmacy records to enforce drug laws.[530] And the USA-PATRIOT Act permits the FBI to access your information without notice to you.[531]

Some laws aimed at medical privacy have conflicted with the First Amendment right of free speech. That's why the Supreme Court recently struck down a Vermont statute that prohibited pharmacies from selling information about doctors' prescribing habits to drug-company salespeople who could use it to push their brand-name drugs.[532] The law targeted only those particular speakers, and thus ran afoul of requirements that any restriction on free speech be neutral as to its content.[533]

Notably, medical records are unique because *some* medical records should remain forever secret—those that record communications with your doctor in order to get medical treatment. There are federal and state privileges protecting communications with therapists, psychologists, psychiatrists, counselors of battered women and sexual assault victims, doctors, and other health care providers.[534] There are exceptions, of course, as when disclosure is necessary to protect someone from serious physical harm.[535] And there are other instances in which you might choose to waive the privilege because the communication pertains to an issue in litigation, as in a malpractice suit or an insanity defense.

School records

Under the federal Family Educational Rights and Privacy Act of 1974,[536] schools will not receive federal funding unless they comply with certain provisions requiring them to grant parents access to their children's "education records," which are defined as, "records, files, documents, and other materials" that "contain information directly related to a student" and that "are maintained by an educational agency or institution or by a person acting for such agency or institution."[537] (This definition excludes peer-reviewed work, among other things.[538]) The statutory rights shift to the students themselves when they're eighteen.[539]

The school mustn't disclose these education records without consent, except to school officials of the current school and any school where the student hopes to attend, with some exceptions,[540] such as certain social workers.[541] This may mean that a student's grades might be kept from an employer.[542]

That said, the statute and regulations do not grant students a right to sue.[543] Instead, a remedy for any violation may only be sought from an administrative board.[544] An analogous state law grants parents the right to see student medical and educational records, although some counseling may be held privileged even from parents.[545]

Another federal funding law—the No Child Left Behind Act of 2001—ensures that military recruiters receive special access to high-school students. It denies funding for any school that doesn't give them "access to secondary school students[']names, addresses, and telephone listings."[546] And it specifically overrides a law in Connecticut that would have prohibited release of this information to recruiters.[547] While it has a provision for parents to request that the information be kept from recruiters without their prior consent,[548] commentators say that parents often don't know how to invoke this provision, and the law is criticized as targeting people especially vulnerable to coercion.[549]

What's worse, despite these opt-out provisions, there are problems with sharing the personal information of those students who elect to take the Armed Services Vocational Aptitude Battery, a military aptitude test. This test is not covered by the federal educational privacy law. Students taking the test may therefore —if the school's policy is to share the information with the military— find that recruiters get to see information from the tests, which might include the personal contact information we've already mentioned as well as Social Security numbers.[550] Compounding this, there have been many reported incidents of recruiters pressuring students into taking these military aptitude tests without adequate disclosure of what the test was about, or in some cases, falsely claiming it was mandatory.[551]

More miscellany

Each of the following laws was written in response to some decision or event that brought the specific privacy concern addressed to the attention of the public. They illustrate the ad-hoc nature of privacy laws and are worth discussing for that reason alone.

Press

The Privacy Protection Act of 1980 was written to protect newspapers and other publishers from government intrusion by requiring probable cause that the publisher is committing a crime related to the materials sought, as with child pornography, or that seeking them is necessary to prevent someone from being seriously hurt or worse.[552] It effectively overrules a holding by the Supreme Court of the United States that searching a newspaper office doesn't require that anyone there be suspected of a crime.[553]

Videos

When President Ronald Reagan nominated Judge Robert Bork of the U.S. Court of Appeals for the District of Columbia Circuit to sit on the Supreme Court of the United States, a journalist accessed his video rental records hoping, perhaps, to embarrass him with a revelation that he'd rented pornographic movies (he hadn't).[554] Congress was so impressed with the incident that it passed the Video Privacy Protection Act of 1988 to render confidential what movies you've rented.[555] Recently updated to conform to the realities of the internet,[556] it had been interpreted broadly enough to include modern ways of renting movies, too, as with Netflix, which has already been held to the law.[557] Connecticut has its own analog.[558]

Entertainment

We've already mentioned the Connecticut Communications Consumer Privacy Act, which forbids electronic entertainment companies from spying on you; it also prohibits them from disclosing without consent your name, subscriber information, or "viewing habits."[559] Anyone who breaks this law may be fined and sued.[560] A federal law, the Cable Communications Privacy Act of 1984, forbids cable companies from sharing your personally identifiable information without your consent.[561]

Internet

Many of the laws we've just discussed apply to the internet as much as anything else. For example, Section Five of the Federal Trade Commission Act applies to online privacy policies, the Video Privacy Protection Act to Netflix, and (see the section titled

Listening to What We Say) the Electronic Communications Privacy Act of 1986 to interception of emails and the like. But there are some more recent laws that are tailored for the internet, including some to protect online privacy. The Children's Online Privacy Protection Act of 1998, for example, requires clear privacy policies, notices to parents and the right to delete their kids' information, choices and transparency for parents, prohibitions on requiring greater information as a condition of use, and confidentiality.[562] And there's a pending policy initiative by the FTC, the Do Not Track initiative, to keep certain sites from following you.[563] Some laws, however, are meant to take internet privacy away, such as the Digital Millennium Copyright Act, which is intended to expose sites and users that infringe on intellectual property.[564]

The theory behind the Children's Online Privacy Protection Act and many other privacy laws is, according to some commentators, based on the principle that some information may be identifiable while other information remains anonymous.[565] But, largely because every computer that uses the internet has an IP, or internet protocol, address, every computer can be tracked and much information that seems anonymous can be decoded.[566] (It's even possible to tell from a printed page what printer it came from.[567]) Because the laws don't adequately take this and other considerations into account, it may be necessary to rethink how these laws work.[568]

Yet preserving your privacy on the internet may have more to do with knowing how to use it, and your computer, than it does with a summary of the statutes. Among other things, you should actually read the privacy policies that frequently confront us but which we then ignore. These will tell you, among other things, that your email might just be mined by your email provider to tailor ads to your taste.[569] And they'll tell you with whom you're sharing all those social media posts that many of us make.[570] (If these providers and websites mislead you with their privacy policies, or if they don't follow them, Section Five of the FTC Act described above may provide a remedy.) Privacy policies aside, you should also learn about software that helps you enhance your privacy online by blocking cookies and spyware and other programs that are sent to your computer to track its use of the internet. You would be wise to

avoid responding to any SPAM, which may be used merely to PHISH for your personal information (a technical but self-evident term). That said, there is some law on SPAM, including the Controlling the Assault of Non-Solicited Pornography and Marketing (called CAN-SPAM).[571] For SPAM sent to a mobile device, there's the Telephone Consumer Protection Act of 1991.[572] For what it's worth, a Connecticut law forbids spammers from hiding or falsifying their return addresses or routing information.[573]

Technological advice is pretty well beyond our ken, but we leave you with one common-sense piece of advice: whatever you write on the internet may have perpetual existence. So you must not give up your own private information unless you've considered the risks very carefully.

Identity theft

What if, despite these laws and your best efforts to keep your personal identifying information private, someone gets hold of it, pretends to be you, and causes you harm? On the federal level, there are certain criminal statutes barring identify theft by any "means of identification" including Social Security numbers and other personal data, fingerprints, biometric data, electronic identifiers and all sorts of other things.[574] And the FTC is charged with protecting consumers from such theft. The FTC advises victims to report the incident to all three credit bureaus, close any tainted accounts, report the crime to the police, and file an FTC complaint.[575] Connecticut law defines identity theft as using somebody else's personal identifying information—such as Social Security number, birth date, driver's license, bank accounts, fingerprints or biological data—to get things or services.[576] It's a felony in Connecticut, and also may be the basis for a civil suit.[577]

Again, common sense measures will help, such as shredding material with private information on it. (By the way, police may freely look through your trash, too, without its being a search.[578])

Automobile event data recorders (black box)

The internet is hardly the only technology with privacy implications that have escaped the attention of lawmakers. Unfortunately, it seems almost as if privacy is the last thing that rule-makers and legislators

think about when they're writing laws. On the federal level, a good example is the automobile event data recorder (like an airplane's black box, but for a car) that's probably in your new vehicle. These boxes provide data to recreate any accident and, to this end, record all sorts of things, including your speed and trajectory.[579] That might serve you well if you want to show that a wreck wasn't your fault. But it may also reveal things about yourself and habits that you don't wish to share. Unfortunately, the regulations promulgated by the National Highway Traffic Safety Administration (NHTSA) are all but silent on privacy issues.[580] The state, however, has a law to keep the data from these boxes confidential, forbidding disclosure without consent or a warrant.[581]

RFID

Radio-frequency identification chips are yet another technology that's growing ever more commonplace despite the potential to reduce our privacy.[582] These RFID chips are tiny devices that contain an identification code that can be read by a scanner.[583] Many of them are so-called passive chips, which have no batteries and draw power from the scanner that reads them.[584] They can be read from only a short distance away.[585] Others—such as the ones in your E-ZPass, if you have one—have a battery and emit a signal that can be read from a distance.[586]

RFID chips, mostly of the passive kind, have already found uses in the military for moving and tracking supplies, among retailers for shipping and tracking inventory, in libraries for cataloging books and in car keys for keyless entry. They are starting to turn up in fobs to turn off house alarms and even for insertion into the human body as a medical identity card or as keys to a house.[587] Incredibly, medically implanted RFIDs have already been used for such frivolous things as a ticket to a nightclub.[588] And in addition to this long list of uses, RFID chips are in new U.S. passports.[589]

Indeed, there's been a huge push to put RFID into identification cards, such as driver's licenses, in the years following the terrorist attacks of 2001. (IDs generally have become more important in recent years, and many states—but not Connecticut—require a photo ID to vote.[590]) The most publicized such effort arose from the plan to

create national identity cards, or, more accurately, national standards for identity cards issued by states. That was the 2005 REAL ID Act, which requires machine reading standards for driver's licenses and the like.[591] RFID fits the bill, although the Department of Homeland Security does not require RFID for REAL ID compliance. That agency has, however, incorporated RFID into driver's licenses under its Western Hemisphere Travel Initiative. Anyway, there are many states that have refused to comply with REAL ID (Connecticut lets you opt out) and Connecticut does not issue RFID-tagged licenses under the Western Hemisphere Travel Initiative.[592] In Connecticut, an effort to require a study of using RFID for vehicle registration failed in 2012.[593]

What will happen with RFID technology remains to be seen. Whether it will be possible to read these chips to track your location, or to inventory the things you own, is a matter of serious concern.[594] To some extent this involves such technical matters as the security of the codes on them, which have sometimes failed.[595] And if the code of an RFID chip in your passport is tracked or hacked, you can imagine that the most serious consequences might follow.[596]

Legislation

There are several places where the holes must be fixed on both the federal and state level, even where there are comprehensive laws. As we've already mentioned in other sections of this guide, the claimed extraordinary power to search or seize almost any records held by a third party under the USA-PATRIOT Act must end. Moreover, the lax requirements of the Stored Communications Act, which applies among other things to our internet information, should be replaced by warrant requirements. All personal identifying information held by third parties, in whatever form, should be kept confidential and only on the terms we choose to share it. Nor should any third party be compelled to give up our information without a warrant or lawful subpoena.

Several new technologies are not yet being regulated in Connecticut to address privacy concerns. The most important of these is RFID technology, which looks to be one of the biggest threats to our privacy in the immediate future. Here, we believe that

there must be studies of how this technology will be used, and how it works.[597] There must be guidelines and laws on both levels to forbid secret databases that collect personally identifying information from RFID.[598] Never should RFID tags be sold in consumer products without a buyer's informed consent, whether the tags are disabled or not.[599] There should be limits on what information may be collected by private parties and strict compliance with the terms to which consumers have agreed.[600] Nor should law enforcement be permitted to track or otherwise collect information on people with RFID, whether it's from a system that authorities deploy or from a third party, without a probable-cause warrant. And the legislation should be broad enough to encompass all similar technology that may in the future be used to tag us. Meanwhile, we will continue to oppose legislation aimed at using RFID chips to identify or track Connecticut drivers or vehicles.

Finally, we also aim to forbid certain very specific practices that have recently come to light. For example, standardized military testing in Connecticut high schools has been an increasing problem because students taking the test have no control over the privacy of their scores and their accompanying personal information. Instead, the schools have the choice whether to share the students' information. We therefore have proposed legislation to require all the schools in the state to leave the choice to the kids and their parents.

PRIVACY IN OUR PERSONS

And so we come to the final section of our discussion, devoted to the zone of privacy around one's physical person. Here, we'll explore what freedoms you may have from strip searches and their equivalents—from being touched, fingerprinted and subjected to drug testing (we've already talked about that at work), as well as from having your DNA collected and shared in databases and from being told what medical procedures you may have done on your own body.

Strip searches

There's no question that forcing you to get naked in order to look your body over for evidence is a search. The only question is when it's reasonable. And you might be surprised to find out that the Supreme Court of the United States held in *Florence v. Board of Chosen Freeholders of the County of Burlington* that someone who's arrested and detained in the general population of a jail may be strip-searched, even if the arrest is for a minor crime and there is no individualized suspicion the detainee has drugs or a weapon.[601] Indeed, the Court rendered this rule in a case where a man was pulled over in traffic and detained on account of a warrant for an unpaid fine (separate concurrences explain that it was critical to the five-to-four majority that the arrest was for an outstanding warrant and not just a traffic violation, and that there was no choice but to put the detainee in the general population of the jail).[602] Writing that it would be "unworkable" to forbid the search of anyone admitted to jail without individualized suspicion, the Court explained that jail administrators had legitimate interests in finding any injuries or health problems and locating any tattoos that might set off gang violence, as well as finding drugs and weapons.[603] This despite statistics from a different state showing that 23,000 strip searches of jail detainees yielded five cases where contraband was found.[604]

In Connecticut there's a statute that provides greater protection, at least for certain people arrested for minor crimes. That statute says, "No person arrested for a motor vehicle violation or a misdemeanor shall be strip searched unless there is reasonable belief that the individual is concealing a weapon, a controlled substance or

contraband," and it requires arresting officers in all cases to obtain a warrant before conducting a "body cavity" search of any opening but the mouth.[605] (Connecticut courts have decided that reasonable suspicion is constitutionally required for strip searches after arrests for felonies or misdemeanors.[606] Because the *Florence* holding applies only to detention in the general population of a jail, those rulings may remain otherwise untouched.) The statute's protection cuts off "when the person is remanded to a correctional institution pursuant to a court order."[607] Florence himself was detained on a bench warrant to compel payment of the fine, a fact that limits the reach of the Court's holding in cases where there has been no judicial approval of the detention. Still, this state law will ensure that Connecticut police may not conduct suspicionless strip searches of anyone arrested for minor crimes and detained without an order from a judicial officer.

As the law now stands, juvenile detainees, even those who haven't been charged with a crime, may be strip-searched on their initial intake to a detention facility in Connecticut without any suspicion—although such searches may not be conducted repeatedly thereafter without reasonable suspicion of contraband.[608] That's largely for the children's own protection, say the courts, since the state assumes special responsibility for them.[609] This doesn't extend to every child in the state's care: a school official can't conduct a strip search of a student without reasonable suspicion of danger, or a specific reason to believe drugs (or the like) are hidden intimately on her body.[610] Other searches of students need only be reasonable under the circumstances[611]—this last is a ruling that, by the way, has been too broadly interpreted by certain school administrators who seem to think that the Fourth Amendment doesn't apply to them at all.

TSA scanners

Recently there's been another kind of strip search that many of us endure every time we board a plane—unless we choose instead to be patted down—and that's the "virtual strip search" that occurs when we have to step through the Transportation Security Administration's scanners.[612] These scanners, as probably everyone knows by now, are capable of revealing almost every detail of your body (although the agency has offered assurances that the newest software blurs

faces and genitals).[613] And the alternative of being patted down instead may be, for some, no choice at all.[614] Fortunately, the TSA has announced its intention to remove the most invasive scanners in favor of something that shows a less revealing image.[615]

But removal of some machines will not eliminate the risk to civil liberties; after all, there are technologies yet to come. And courts have so far largely approved searches of this kind, calling them administrative searches, which, because they're done for public safety and not to find a criminal, don't violate the Fourth Amendment.[616] Instead, say the courts, they're like traffic stops that are conducted on everyone in a certain area merely to ask questions about a nearby accident.[617] It's even sometimes said that, for international travelers, there's a border exception for warrants.[618] (Physical intrusions aren't our only concern with the TSA: we are also deeply troubled by that agency's recent announcement of a profiling project based on collecting a slew of personal information about travelers.[619]) Because these are done under federal jurisdiction, Connecticut law has nothing to say about it.

Drug testing

Requiring someone to urinate into a cup for a drug test is a search under the Fourth Amendment and requires a warrant if the purpose is to uncover a crime.[620] On the other hand, a governmental authority may subject individuals to such testing without warrants and even without any individualized suspicion if doing so satisfies a special need of a particular government program that's distinct from ordinary law enforcement.[621] To determine whether the search is reasonable, the individual privacy interest at stake must be carefully evaluated and balanced against the needs of the government.[622] Such suspicionless drug tests are most likely to be permitted where there are privacy protections in place and the only consequence is something akin to the denial of government benefits rather than a criminal sanction.[623] Thus, the Supreme Court has held that the government may impose suspicionless drug tests on railroad employees involved in wrecks or safety infractions because of the compelling need for safety[624] and on certain customs employees because of safety and the need to maintain law enforcement officers' fitness and integrity.[625] But, because there was no real issue of public

safety, the Supreme Court forbade suspicionless drug testing as a condition of running for public office.[626] And the Court held that suspicionless testing of pregnant women for cocaine use by a state-run hospital violated the Fourth Amendment because the results were used for a law-enforcement purpose.[627]

Drug testing in public schools has its own special considerations. The Supreme Court of the United States has held that high school athletes have a lower expectation of privacy because they've agreed to participate in programs that require them to shower and change with each other, and the like.[628] Consequently, in light of the special needs of deterring drug use by children (which had nothing to do with law enforcement), these students may be subjected to random drug testing.[629] And the Court applied this holding to middle and high school students who've signed up for other extracurricular activities.[630] Even so, that balance with special needs does not allow for drug testing without suspicion if the purpose of the search is to uncover crime.[631]

The state may write its own laws to decide whether to subject students to such testing and those, of course, may grant greater protection than the federal constitutional standard. Unfortunately, as it stands, it's left up to each district to decide whether to subject their students to this sort of invasion of privacy.[632] Also, school boards decide locally whether to employ drug-sniffing dogs on the unattended property of students.[633]

Fingerprinting

It has been argued that there's no expectation of privacy in your fingerprints because you leave them all over the place.[634] Still, the police may not detain you and force you to give a sample without implicating the Fourth Amendment.[635] We have yet to see whether such rulings will apply to those sophisticated new surveillance cameras that can record your fingerprints at a distance without you ever knowing it.[636]

Meanwhile, there are federal statutes that say when your fingerprints may be taken. These apply to federal employees who are subject to background checks, immigrants, migrant laborers, commodity traders, mortgage lenders, bankers, importers of

explosives and guns, transporters of hazardous materials, people who work on aircraft, workers at long-term care facilities, people who work in atomic energy, those charged with the care of children, registered sex offenders and prisoners, including juveniles.[637]

Connecticut has its own statutes to say who may or may not take your fingerprints. Police, for example, may take fingerprints if they arrest you, although you have a right to demand samples back if you're not convicted.[638] Otherwise, the state police bureau of identification keeps the fingerprints.[639] And they're kept for prisoners and sex offenders who must register.[640] Additionally, you must submit fingerprints and undergo a criminal background check to buy a handgun or apply for a handgun permit.[641] Fingerprinting is also a condition of taking certain jobs, such as public school teacher, DMV worker, employee of the Bureau of Rehabilitative Services, taxi driver and bus driver. It's also a condition of being licensed by the state bar or as a driving instructor, pawn broker, bail bondsman, private security worker, private detective or mortgage lender. It's also required of those who use or transport explosives, run a private employment agency or organize a bank or credit union.[642] In short: loads of things.

DNA testing

Like a fingerprint, your DNA is a unique identifier. But, unlike fingerprints, taking a DNA sample gives more than mere identifying information. DNA might reveal things about your health and other things that you may not wish to share.[643] And there's no doubt that requiring someone to provide a DNA sample for analysis is a search, protected by the Fourth Amendment.[644]

Some, but not all, courts have upheld searches collecting DNA from those who've been charged with felonies, even though they hadn't yet been convicted, and there's a pending case on the matter in the Supreme Court of the United States.[645] Meanwhile, such searches are authorized for people who have been arrested for or convicted of certain felonies by federal law under the DNA Fingerprint Act of 2005.[646] In Connecticut, all those convicted (or found not guilty by reason of insanity) of felonies and certain crimes against children and sex crimes must give a DNA sample as a condition of their

sentence or custody.[647] Convicted felons who haven't given the sample and who get arrested again for certain serious felonies must give the sample upon arrest.[648] It is a felony to refuse.[649] The DNA information is stored in a data bank where there are some safeguards against unauthorized dissemination, and there is a right to have it expunged if the conviction or finding of not guilty by reason of insanity is overturned.[650]

Other federal and state statutes forbid discrimination based on the information acquired through DNA testing.[651] And a state statute forbids employers from taking a DNA sample during hiring or from discriminating on the basis of DNA.[652]

Reproductive and sexual privacy

Connecticut has had laws on the books over the years that offend the notion of reproductive and sexual privacy implied by the Constitution of the United States. In fact it was a Connecticut law banning all contraception that the Supreme Court of the United States invalidated while stating that privacy right for the first time.[653]

At that time, our state also had statutes that outlawed all abortions except to save the mother's life.[654] But then *Roe v. Wade* struck down another state's abortion laws. The Court in that case reasoned that in the first trimester a woman's right to privacy must permit her choice to have an abortion, in the second the state's interest in preserving life must be balanced against that privacy right, and in the third, the state's interest wins except in cases of the life and health of the mother.[655] In a later case, *Planned Parenthood of Southeastern Pennsylvania v. Casey*, the Court revisited that ruling and refined it to say that laws must not place an "undue burden" on women who seek an abortion before viability.[657] And all laws that were inconsistent with that had to be rewritten.

Now Connecticut permits abortions before the fetus's viability and outlaws abortions afterward except when the mother's life or health is at risk.[658] Viability isn't defined by the statute, but it means the point at which the fetus can survive outside the womb.[659] The law also requires regulations for abortion procedures including pre-operation counseling, and it states requirements for counseling of minors under sixteen who undergo abortions, mandating that the

doctor tell them about alternatives to abortion.[660] And it forbids the state school system from teaching "abortion as an alternative to family planning."[661]

Legislation

Simply put, it's time to roll back much of the suspicionless and invasive probing to which we're all subjected. Although the TSA has announced that it will stop using its most invasive body scanners, legislation should be put in place to protect us from other such unnecessarily intrusive searches. And, while we're pleased that Connecticut statutes don't permit strip searches as often as the Supreme Court of the United States would, it's time to revisit when and why strip searches should be conducted. What's more, the state should pass laws to limit when school students may be subjected to drug testing. Meanwhile, we'll continue to oppose all efforts to increase the collection of DNA samples from people who are arrested for, but not convicted of, crimes, and to work for the repeal of the laws that already permit such collection.

CONCLUSION

We hope that this guide has been a useful introduction to the privacy issues that face us in Connecticut, and that we've identified the most important gaps in the law and new technologies that require the most urgent action. Indeed, the time for such action has never been more pressing than now, for this is a critical time for privacy law. As we've said, the changes to technology are moving so quickly that, if we don't act soon, our current expectations of privacy may forever change before we have the chance to preserve them. We're determined not to let that happen, and hope that you share that determination, too.

NOTES

[1] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev 193, 193-95 (1890) (citation omitted) (internal quotation marks omitted).

[2] *Id*. at 195-217.

[3] *See* Griswold v. Connecticut, 381 U.S. 479, 510 n.1 (1965) (Black, J., dissenting) (discussing the development of state-law causes of action inspired by Warren's and Brandeis's writing).

[4] *See* Ellen Alderman & Caroline Kennedy, The Right to Privacy 155 (1995).

[5] U.S. Const. amend. IV; Conn. Const. art. 1, § 7.

[6] Katz v. United States, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring); *see also* Kyllo v. United States, 533 U.S. 27, 33 (2001) (explaining that this test arose from Justice Harlan's concurrence); State v. Gonzalez, 898 A.2d 149, 154 n.11 (Conn. 2006) (same).

[7] *See Griswold*, 381 U.S. at 482-86 (majority opinion).

[8] N.Y. Civil Liberties Union, Who's Watching? (2006), *reprinted in* Are Privacy Rights Being Violated? 10-16 (Ronald D. Lankford, Jr. ed., 2010); *see, e.g.*, Richie Rathsack, *Police Setting Up Surveillance Camera System in Downtown Meriden*, Meriden Record-Journal, Oct. 23, 2012, http://www.myrecordjournal.com/meriden/article_0a9d4eb4-1d36-11e2-a93d-001a4bcf887a.html; *First 'Intelligent Security Cameras' with Facial Recognition Available in North America from Gadspot*, PR Newswire, Oct. 10, 2012, http://www.prnewswire.com/news-releases/first-intelligent-security-cameras-with-facial-recognition-available-in-north-america-from-gadspot-173477531.html; Cadie Thompson, *How Facial Recognition Technology Could Help Catch Criminals*, CNBC.com (Apr. 19, 2013, 2:52 PM), http://www.cnbc.com/id/100656156.

[9] Matthew Kauffman, *Police Keeping Data from License Plate Scans*, Hartford Courant, Feb. 21, 2012, http://articles.courant.com/2012-02-21/news/hc-aclu-license-plate-scans-0222-20120221_1_license-plate-scans-police-cars.

[10] Brendan Sasso, *Police Made 'Startling' 1.3 Million Requests in 2011 for Cellphone Data*, Hillicon Valley, Hill's Tech. Blog (July 9, 2012, 10:07 AM), http://thehill.com/blogs/hillicon-valley/technology/236683-startling-rise-in-police-requests-for-cellphone-data.

[11] Antonio Regalado, High Stakes in Internet Tracking, MIT Tech. Rev. (June 4, 2012), http://www.technologyreview.com/news/428044/high-stakes-in-internet-tracking/.

[12] Scott Shane, *Data Storage Could Expand Reach of Surveillance*, Caucus, Pol. & Gov't Blog, N.Y. Times (Aug. 14, 2012, 5:50 PM), http://thecaucus.blogs.nytimes.com/2012/08/14/advances-in-data-storage-have-implications-for-government-surveillance/.

[13] *Id*.

[14] *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) (noting that Congress and the states haven't addressed GPS).

[15] *See* Orrin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 875 (2004).

[16] We are grateful for the work of the National American Civil Liberties Union and others, like The Electronic Frontier Foundation, *see* Electronic Frontier Found., http://www.eff.org (last visited Feb. 23, 2013), which provided excellent background to aid our identification of privacy issues in Connecticut.

[17] Edmonson v. Leesville Concrete Co., 500 U.S. 614, 619 (1991) (explaining that the Constitution of the United States applies only to government action, with few exceptions like the Thirteenth Amendment abolishing slavery).

[18] *See, e.g.*, Leydon v. Town of Greenwich, 777 A.2d 552, 578 (Conn. 2001).

[19] Bailey v. United States, No. 11-770, 2013 WL 598438, at *4 (U.S. Feb. 19, 2013); Payton v. New York, 445 U.S. 573, 576 (1980).

[20] U.S. Const. amend. IV.

[21] *See, e.g., Jones*, 132 S. Ct. at 948. *See generally* ALDERMAN & KENNEDY, *supra* note 4, at 23 (providing a discussion of these principles for the layperson).

[22] Florida v. Jardines, No. 11–564, 2013 WL 1196577, at *6 (U.S. Mar. 26, 2013); *Jones*, 132 S. Ct. at 949-54.

[23] *See Jones*, 132 S. Ct. at 949-50; *Jardines*, 2013 WL 1196577, at *1-6.

[24] *Jardines*, 2013 WL 1196577, at *4 (citation omitted) (internal quotation marks omitted); *accord Jones*, 132 S. Ct. at 953 (citing Oliver v. United States, 466 U.S. 170 (1984)).

[25] *Katz*, 389 U.S. at 360-61 (Harlan, J., concurring); *see also Jardines*, 2013 WL 1196577, at *6 (explaining that this test supplements the trespass test); *Jones*, 132 S. Ct. at 950 (quoting Justice Harlan's concurrence in *Katz*); *Kyllo*, 533 U.S. at 33 (applying test).

[26] *Kyllo*, 533 U.S. at 33; *Katz*, 389 U.S. at 360-61 (Harlan, J., concurring).

[27] *E.g., Jardines*, 2013 WL 1196577, at *1-6. These marijuana examples consequently reappear in other secondary sources. *See, e.g.*, ALDERMAN & KENNEDY, *supra* note 4, at 23-30.

[28] *See Jardines*, 2013 WL 1196577, at *1-6.

[29] *Jardines*, 2013 WL 1196577, at *6; *cf. Payton*, 445 U.S. at 589-90 (noting elevated privacy in the home).

[30] *Cf. Kyllo*, 533 U.S. at 31-33; Texas v. Brown, 460 U.S. 730, 740 (1983) (plurality).

[31] *Cf.* Florida v. Riley, 488 U.S. 445 (1989) (plurality); California v. Ciraolo, 476 U.S. 207 (1986).

[32] *See Kyllo*, 533 U.S. at 31-33.

[33] *See id.* at 31-33; *Ciraolo*, 476 U.S. at 213.

[34] *See* United States v. Knotts, 460 U.S. 276, 281 (1983).

[35] *Cf. Oliver*, 466 U.S. at 173-74.

[36] *Jones*, 132 S. Ct. at 953 (citing *Oliver*, 466 U.S. at 176-77).

[37] *Katz*, 389 U.S. at 348-49; *id.* at 360-61 (Harlan, J., concurring).

[38] *Id.* at 352-353 (majority opinion).

[39] *Id.* at 361 (Harlan, J., concurring).

[40] *Kyllo*, 533 U.S. at 33; Terry v. Ohio, 392 U.S. 1, 9 (1968).

[41] United States v. Miller, 425 U.S. 435, 443 (1976), *superseded by statute*, 12 U.S.C. § 3401 (2006), *as recognized in* Chao v. Cmty. Trust Co., 474 F.3d 75, 83 (3d Cir. 2007).

[42] *See id.*

[43] 12 U.S.C. §§ 3401-3421 (2006 & Supp. V 2011); *see Chao*, 474 F.3d at 83.

[44] *Kyllo*, 533 U.S. at 32.

[45] *See* Kentucky v. King, 131 S. Ct. 1849, 1856 (2011).

[46] Johnson v. United States, 333 U.S. 10, 13-14 (1948).

[47] *See* Illinois v. Gates, 462 U.S. 213, 238 (1983).

[48] U.S. Const. amend. IV; Groh v. Ramirez, 540 U.S. 551 (2004). In addition to these basic constitutional requirements, there are other laws that establish the procedure to obtain a warrant. Fed. R. Crim. P. 41; Conn. Gen. Stat. §§ 54-33a—54-33n (2013).

[49] *See* Illinois v. Rodriguez, 497 U.S. 177, 186 n.* (1990).

[50] *See* Florida v. Bostick, 501 U.S. 429 (1991); *id.* at 440-51 (Marshall, J., dissenting).

[51] *Cf.* Coolidge v. New Hampshire, 403 U.S. 443, 487-90 (1971); *Rodriguez*, 497 U.S. at 179.

[52] *King*, 131 S. Ct. at 1853-54.

[53] *See* United States v. Cisneros-Gutierrez, 598 F.3d 997, 1004 (8th Cir. 2010).

[54] Missouri v. McNeely, No. 11–1425, 2013 WL 1628934 (U.S. Apr. 17, 2013).

[55] *See, e.g.*, California v. Acevedo, 500 U.S. 565 (1991); Schmerber v. California, 384 U.S. 757, 768-70 (1966). *Schmerber* is another drunk-driving case, and a famous one. *See, e.g.*, Alderman & Kennedy, *supra* note 4, at 29.

[56] Arizona v. Gant, 556 U.S. 332, 344-45 (2009).

[57] *King*, 131 S. Ct. at 1858.

[58] *See* U.S. Const. amend. IV.

[59] *Terry*, 392 U.S. 9-31.

[60] *Id.*; State v. Oquendo, 613 A.2d 1300, 1320 (Conn. 1992).

[61] *See, e.g.*, *Terry*, 392 U.S. at 27.

[62] *Id.* at 22-23.

[63] *See id.* at 23-28.

[64] *See* Davis v. United States, 131 S. Ct. 2419, 2426-29 (2011).

[65] *Id.* at 2426.

[66] *See, e.g.*, Hudson v. Michigan, 547 U.S. 586, 591-92 (2006).

[67] *Id.* (cites and internal quotation marks omitted).

[68] *Johnson*, 333 U.S. at 14; *see also Davis*, 131 S. Ct. at 2426-27 (explaining purpose of exclusion as deterrence). There are multiple exceptions to the exclusionary rule, including the good-faith exception, which applies when the police reasonably believe their actions are lawful. *Davis*, 131 S. Ct. at 2427-28. A federal court doesn't have to apply the exclusionary rule on collateral review—that is, a second action brought after a conviction to challenge its constitutionality, often called habeas corpus—if the person convicted had a full and fair opportunity to press his Fourth Amendment claim during the original prosecution. Young v. Conway, 698 F.3d 69, 85 (2d Cir. 2012).

[69] A statute, 42 U.S.C. § 1983 (2006 & Supp. V 2011), allows you to sue a person acting under color of state law (as it's said) for violation of constitutional rights. Typically, a suit for money damages under the statute must be against that person in his individual capacity. Ying Jing Gan v. City of New York, 996 F.2d 522, 529 (2d Cir. 1993). That's because the Eleventh Amendment to the Constitution of the United States means that neither a state nor a state employee acting in his official capacity may be sued for money damages. *Id.* Even so, the Eleventh Amendment generally doesn't bar a suit against a defendant in his official capacity if it's for an injunction, which is an order saying that you must do or stop doing something. Fulton v. Goord, 591 F.3d 37, 45 (2d Cir. 2009).

And so you may sue to enjoin enforcement of an unconstitutional statute. Also, there is a narrow exception for a claim against a municipal or similar government entity, or an employee in his or her official capacity, for a violation arising from a policy or custom of the government entity. Monell v. Dep't of Soc. Servs., 436 U.S. 658, 691 n.33 (1978). Federal employees may not be sued under section 1983, yet the Supreme Court of the United States carved out a rule to permit similar such suits under the same rules. Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388 (1971).

There are various immunities available to defendants under both sets of laws. Judges and prosecutors are usually immune from suit, so long as they stick to their jobs. Stump v. Sparkman, 435 U.S. 349, 359 (1978); Imbler v. Pachtman, 424 U.S. 409, 431 (1976). Police often defend a suit based on qualified immunity. That doctrine says that the defendant may escape liability if the constitutional right violated wasn't clearly established and the defendant reasonably believed that he wasn't violating any constitutional right. Russo v. City of Bridgeport, 479 F.3d 196, 211 (2d Cir. 2007).

It should be noted that there are difficult issues of when the time to file a suit for damages arising from a Fourth Amendment violation begins to run, which is usually when it happens. Wallace v. Kato, 549 U.S. 384 (2007); Heck v. Humphrey, 512 U.S. 477 (1994).

[70] Townes v. City of New York, 176 F.3d 138 (2d Cir. 1999).

[71] Conn. Const. art. 1, § 7.

[72] State v. Jenkins, 3 A.3d 806, 839-40 (Conn. 2010).

[73] *See* United States v. Delaporte, 42 F.3d 1118, 1119-20 (7th Cir. 1994); United States v. Miller, 14 F.3d 761, 762-63 (2d Cir. 1994). *See generally* Advisory Comm'n on Intergovernmental Relations, State Constitutions in the Federal System 69-76 (July 1989), *available at* http://www.library.unt.edu/gpo/acir/Reports/policy/a-113.pdf (exploring the complex interaction between state and federal governments in successive prosecutions). One example of when state law may be relevant to a federal prosecution is when evidence was originally obtained pursuant to warrants issued by

state authorities under state standards; in such a case the warrants' validity is a question of state law. *See, e.g.*, United States v. Manfredi, 488 F.2d 588, 598 (2d Cir. 1973).

[74] *See* State v. Legrand, 20 A.3d 52, 66-67 & n.16 (Conn. App. Ct. 2011).

[75] *Jenkins*, 3 A.3d at 840.

[76] *See* State v. Davis, 929 A.2d 278, 302 (Conn. 2007).

[77] *See, e.g.*, State v. Lamme, 563 A.2d 1372, 1375 (Conn. App. Ct. 1989), *aff'd on other grounds*, 579 A.2d 484 (Conn. 1990).

[78] *Griswold*, 381 U.S. at 480-86. A wonderful discussion of this right to privacy is found in Alderman & Kennedy, *supra* note 4, at 55-153.

[79] *Griswold*, 381 U.S. at 482-86.

[80] *Id.* at 484-86.

[81] Roe v. Wade, 410 U.S. 113, 152-53 (1973). Federal action is governed by the Due Process Clause of the Fifth Amendment. Cook v. Gates, 528 F.3d 42, 45-60 (1st Cir. 2008).

[82] U.S. Const. amend. XIV, § 1.

[83] Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833 (1992) (modifying *Roe*, 410 U.S. 113).

[84] Carey v. Population Servs., 431 U.S. 678, 684-85 (1977).

[85] *See, e.g.*, Lawrence v. Texas, 539 U.S. 558 (2003). The constitutional right to privacy was the basis for a woman's suit against a police officer who taped her while undressing. Poe v. Leonard, 282 F.3d 123, 138-39 (2d Cir. 2002).

[86] U.S. Const. amend. XIV, § 1; *see, e.g.*, Perry v. Brown, 671 F.3d 1052, 1076-96 (9th Cir. 2012), *cert. granted sub nom.*, Hollingsworth v. Perry, 133 S. Ct. 786 (2012). Equal Protection is a principle that applies to the federal government, as well, by way of the Due Process Clause of the Fifth Amendment. Bolling v. Sharpe, 347 U.S. 497, 499 (1954); United States v. Martinez, 621 F.3d 101, 107 n.3 (2d Cir. 2010).

[87] Whalen v. Roe, 429 U.S. 589, 599-600 (1977); Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 457-60 (1977); Nat'l Aeronautics & Space Admin. v. Nelson, 131 S. Ct. 746, 751-56 (2011). While the Supreme Court has assumed that a right to informational privacy exists without definitely holding that it does, the U.S. Court of Appeals for the Second Circuit has definitely held that such a right exists. Doe v. New York, 15 F.3d 264, 267 (2d Cir.1994). The Connecticut Supreme Court has recognized the right. State v. Russo, 790 A.2d 1132, 1148 (Conn. 2002).

[88] *Cf.* In re Michaela Lee R., 756 A.2d 214, 231-32 (Conn. 2000); Ochs v. Borrelli, 445 A.2d 883, 885 (Conn. 1982).

[89] *See* Ramos v. Vernon, 761 A.2d 705, 727 (Conn. 2000).

[90] *See Griswold*, 381 U.S. at 510 n.1 (Black, J., dissenting) (discussing the development of state-law causes of action inspired by Warren's and Brandeis's writing).

[91] At least one case comes from 1947, but that court didn't decide whether there was a right to privacy in Connecticut. O'Connell v. Hartford Times, 15 Conn. Supp. 85 (1947). That's apparently why courts often trace the history of privacy torts in Connecticut to 1959. *See, e.g.*, Perkins v. Freedom of Info. Comm'n, 635 A.2d 783, 789 n.16 (Conn. 1993) (citing Korn v. Rennison, 156 A.2d 476 (Conn. Super. Ct. 1959)).

[92] Goodrich v. Waterbury Republican-Am., 448 A.2d 1317, 1327-29 (Conn. 1982).

[93] *Id.* at 1329; Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 Cal. L. Rev. 1887, 1890 (Dec. 2010).

[94] *Goodrich*, 448 A.2d at 1329 (formatting altered) (citation omitted).

[95] *See* Bennett v. Connecticut Hospice, 741 A.2d 349, 352 (Conn. App. Ct. 1999) (citing *Perkins*, 635 A.2d at 789-91).

[96] *See Perkins*, 635 A.2d at 789 n.15 (citations omitted) (internal quotation marks omitted).

[97] 3 Restatement (Second) Torts § 652B, *quoted in* Gallagher v. Rapoport, No. CV 960149891S, 1997 WL 240907, at *2 (Conn. Super. Ct. May 6, 1997).

[98] *Id.*

[99] *Id.*

[100] Carey v. Statewide Fin. Co., 223 A.2d 405, 406-07 (Conn. Cir. Ct. 1966).

[101] Birge v. Med. Elec. Distrib., No. 075000540, 2009 WL 1959393, at *1-6 (Conn. Super. Ct. June 5, 2009).

[102] *Gallagher*, 1997 WL 240907, at *1; Wilburn v. Fleet Fin. Group, 170 F. Supp. 2d 219, 242, 255 (D. Conn. 2001). One woman was allowed to press a claim that her employer forced her to reveal that she was menstruating. Garces v. R & K Spero Co., No. CV095025895S, 2009 WL 1814510, at *8-9 (Conn. Sup. Ct. May 29, 2009). Another was allowed to claim that her employer forced her to listen to religious harangues and probed her about her sex life. Guccione v. Paley, No. LLICV054002943S, 2006 WL 1828363, at *2-3 (Conn. Super. Ct. June 14, 2006). Still other claims have involved offensive comments without physical touching. *E.g.*, Slowick v. Morgan Stanley & Co., No. CV054003860, 2006 WL 573926, at *2-3 (Conn. Super. Ct. Feb. 21, 2006); Bonanno v. Dan Perkins Chevrolet, No. CV99-066602, 2000 WL 192182 (Conn. Super. Ct. Feb. 4, 2000).

[103] Turner v. Am. Car Rental, 884 A.2d 7, 11 (Conn. App. Ct. 2005).

[104] *Id.* at 8, 11.

[105] Fiorillo v. Berkley Adm'rs, No. CV010458400S, 2004 WL 1153678, at *1-5 (Conn. Super. Ct. May 5, 2004); United States v. Vazquez, 31 F. Supp. 2d 85, 90-91 (D. Conn. 1998). But another court recognized that following the plaintiff about coupled with other conduct like trespassing and harassing phone calls could amount to an invasion of privacy. Anderson v. Drapp, No. CV030402737, 2003 WL 22205645 (Conn. Super. Ct. Sept. 5, 2003).

[106] Schmidt v. Devino, 206 F. Supp. 2d 301, 309-10 (D. Conn. 2001).

[107] *Bennett*, 741 A.2d at 351-52.

[108] Graff v. O'Connell, No. CV010095518S, 2002 WL 450534, at *5-6 (Conn. Super. Ct. Mar. 5, 2002).

[109] Cavallaro v. Rosado, No. CV054009939, 2006 WL 2949143, at *3-5 (Conn. Super. Ct. Oct. 5, 2006).

[110] *Id.* at *5.

[111] 3 Restatement (Second) Torts § 652C, *quoted in* Gleason v. Smolinski, No. NNHCV065005107S, 2009 WL 2506607, at *4 (Conn. Super. Ct. July 20, 2009).

[112] *Id.*

[113] *Korn*, 156 A.2d at 477-78.

[114] *Id.* at 478. Another court allowed a woman to press a claim that her face was used on a billboard advertising "welfare to work programs" without her consent. Herring v. Radding Signs, No. CV 990427523, 2000 WL 192959 (Conn. Sup. Ct. Feb. 9, 2000). The cases have been unclear about whether commercial appropriation is actionable only when it's offensive to a reasonable person. *See* Venturi v. Savitt, Inc., 468 A.2d 933 (Conn. 1983).

[115] Steding v. Battistoni, 208 A.2d 559, 560-63 (Conn. Cir. Ct. App. Div. 1964).

[116] *Goodrich*, 448 A.2d at 1331.

[117] *Id.*

[118] *E.g.*, Alexandru v. Dowd, 830 A.2d 352, 355 (Conn. App. Ct. 2003); Tarka v. Filipovic, 694 A.2d 824, 828-29 (Conn. App. Ct. 1997); Tucker v. Bitonti, 382 A.2d 841, 843 (Conn. Super. Ct. 1977).

[119] *Goodrich*, 448 A.2d at 1325-27 (internal quotation marks omitted).

[120] *Gleason*, 2009 WL 2506607, at *5-6 (internal quotation marks omitted).

[121] Miller v. News Syndicate Co., 445 F.2d 356, 356-58 (2d. Cir. 1971).

[122] *See Perkins*, 635 A.2d at 789 n.15 (citations omitted).

[123] *Goodrich*, 448 A.2d at 1330.

[124] *Id.*

[125] *E.g.*, Jensen v. Times Mirror Co., 634 F. Supp. 304 (D. Conn. 1986).

[126] Gleason v. Smolinski, No. NNHCV065005107S, 2012 WL 3871999, at *16 (Conn. Super. Ct. Aug. 10, 2012); *Cavallaro*, 2006 WL 2949143, at *7; Senior v. Hartford Fin. Servs. Group, 31 Conn. L. Rptr. 268 (Conn. Super. Ct. 2002); Holmes v. Town of East Lyme, 866 F. Supp. 2d 108, 132 (D. Conn. 2012); Byra-Grzegorczyk v. Bristol-Myers Squibb Co., 572 F. Supp. 2d 233, 257-58 (D. Conn. 2008).

[127] Grigorenko v. Pauls, 297 F. Supp. 2d 446, 448-49 (D. Conn. 2003).

[128] Grossman v. Computer Curriculum Corp., 131 F. Supp. 2d 299, 311-12 (D. Conn. 2000); Pace v. Bristol Hosp., 964 F. Supp. 628 (D. Conn. 1997).

[129] *E.g.*, Sargeant v. Serrani, 866 F. Supp. 657, 667-68 (D. Conn. 1994).

[130] Brown v. Ne. Nuclear Energy Co., 118 F. Supp. 2d 217, 225 (D. Conn. 2000).

[131] Belanger v. Swift Transp., 552 F. Supp. 2d 297, 301-02 (D. Conn. 2008).

[132] *Tucker*, 382 A.2d at 843; *Alexandru*, 830 A.2d at 355.

[133] *Goodrich*, 448 A.2d at 1330-31.

[134] *O'Connell*, 15 Conn. Supp. at 85.

[135] *Sargeant*, 866 F. Supp. at 663-64.

[136] Murray v. Schlosser, 574 A.2d 1339 (Conn. Super. Ct. 1990). This is another famous case. See, e.g., ALDERMAN & KENNEDY, *supra* note 4, at 208.

[137] *Murray*, 574 A.2d at 1339-40 (internal quotation marks omitted).

[138] *Id.* at 1341.

[139] Jonap v. Silver, 474 A.2d 800, 802, 805-06 (Conn. App. Ct. 1984).

[140] Rizzitelli v. Thompson, No. CV095009384S, 2010 WL 3341516, at *6-7 (Conn. Super. Ct. Aug. 2, 2010).

[141] Honan v. Dimyan, 726 A.2d 613, 618-19 (Conn. App. Ct. 1999).

[142] *About Us*, Am. Civ. Liberties Union Conn., http://www.acluct.org/aboutus/ (last visited Feb. 23, 2013).

[143] *E.g.*, *In re* State Police Litigation, 888 F. Supp. 1235, 1271 (D. Conn. 1995), *appeal dismissed*, 88 F.3d 111 (2d Cir. 1996); Singhaviroj v. Town of Fairfield, No. CV054007480S, 2011 WL 1176163, at *14-16 (Conn. Super. Ct. Mar. 09, 2011).

A state law immunizes a state employee unless the act is malicious, reckless, or wanton. Conn. Gen. Stat. § 4-165 (2013). But a political subdivision of the state such as a town may not be liable for intentional torts of its employees, nor forced to indemnify them for those torts. O'Connor v. Bd. of Educ., 877 A.2d 860 (Conn. App. Ct. 2005); Singhaviroj, 2011 WL 1176163, at *14-16. So an employee committing an intentional tort may be sued for money damages only in his or her personal capacity.

But there is an exception to sovereign immunity that permits a person to sue an employee in his official capacity for an injunction—which is an order to do or stop doing something—if that employee exceeds his statutory authority to promote an illegal end. Elec. Contractors, Inc. v. Dep't of Educ., 35 A.3d 188, 224 (Conn. 2012).

These and related issues of governmental liability and immunity are exceptionally complicated. *See* Grady v. Town of Somers, 984 A.2d 684 (Conn. Dec. 22, 2009) (overruling Pane v. City of Danbury, 841 A.2d 684 (Conn. 2004)), *discussed in* Miles v. City of Hartford, 719 F.Supp.2d 207, 216-18 (D. Conn. 2010), *aff'd*, 445 Fed. App'x 379 (2d Cir. 2011).

[144] Snyder v. Phelps, 131 S. Ct. 1207, 1213-14 (2011) (internal quotation marks omitted).

[145] *Id.* at 1213-21.

[146] *Id.*

[147] *See* Brief for American Civil Liberties Union and American Civil Liberties Union of Maryland as Amici Curiae Supporting Respondents, Snyder v. Phelps, 131 S. Ct. 1207 (2011) (No. 09-751), 2010 WL 2811208.

[148] *See, e.g.*, 18 U.S.C. §§ 2510–2522 (2006 & Supp. V 2011); see also Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 Fordham L. Rev. 747, 754 (2005) [hereinafter Solove, *Fourth Amendment Codification*] (discussing code and constitution); Kerr, *supra* note 15, at 850-51.

[149] Conn. Gen. Stat. § 52-570d (2013); State v. McVeigh, 620 A.2d 133, 138-39 & n.17 (Conn. 1993).

[150] Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 Cal. L. Rev. 2007, 2009 (2010).

[151] That's because of the Supremacy Clause, which says:

> This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding.

U.S. Const. art. VI, cl. 2.

[152] *See, e.g.*, Nat'l Fed. of Indep. Bus. v. Sebelius, 132 S. Ct. 2566, 2585-91 (2012) (construing limits of federal power under the Commerce Clause).

[153] *Statement of Rights and Responsibilities*, Facebook, http://www.facebook.com/legal/terms (last updated Dec. 11, 2012); *Google Terms of Service*, Google, http://www.google.com/policies/terms/ (last modified Mar. 1, 2012); *Terms and Conditions of Use*, Barnes

& Noble, http://www.barnesandnoble.com/include/terms_of_use.asp (last visited Feb. 23, 2013).

[154] Robert A. Hillman & Maureen O'Rourke, *Defending Disclosure in Software Licensing*, 78 U. Chi. L. Rev. 95, 103 (2011).

[155] Fed. R. Civ. P. 26(b)(1); 2013 Connecticut Practice Book (rev. 1998), § 13–2.

[156] Fed. R. Civ. P. 26(b)(1); Practice Book, § 13–2.

[157] *See, e.g.*, United States v. Jicarilla Apache Nation, 131 S. Ct. 2313, 2321 (2011); Jaffee v. Redmond, 518 U.S. 1, 3-18 (1996).

[158] *See, e.g.*, *Jicarilla Apache Nation*, 131 S. Ct. at 2321; *Jaffee*, 518 U.S. at 3-18.

[159] *See, e.g.*, Bond v. Utreras, 585 F.3d 1061, 1073 (2009).

[160] *E.g., id.* at 1065.

[161] Buxton v. Ullman, 156 A.2d 508, 514-15 (Conn. 1959); Doe v. Diocese Corp., 647 A.2d 1067, 1070-72 (Conn. Super. Ct. 1994); *e.g.*, Doe v. Yale University, 748 A.2d 834 (Conn. 2000); Doe v. Roe, 717 A.2d 706 (Conn. 1998); Doe v. Dep't of Pub. Health, 727 A.2d 260 (Conn. App. Ct. 1999); Practice Book, §§ 11-20A, 25-59A(h).

[162] Conn. Gen. Stat. §§ 1-215(a), 1-210(b)(3) (2013). Connecticut shares criminal records with the FBI and other states. Conn. Gen. Stat. § 29-164f (2013); Frequently Asked Questions Regarding the National Crime Prevention and Privacy Compact Act of 1998 (Apr. 9, 2013), *available at* http://www.fbi.gov/about-us/cjis/cc/library/compact-frequently-asked-questions.

[163] Conn. Gen. Stat. § 54-142a (2013).

[164] *See* Warren & Brandeis, *supra* note 1, at 195, 206, 208-13.

[165] *Cf.* Rathsack, *supra* note 8; *First 'Intelligent Security Cameras' with Facial Recognition Available in North America from Gadspot*, *supra* note 8; Kauffman, *supra* note 9.

[166] Christopher Hoffman, *Wethersfield To Install School Bus Cameras*, Hartford Courant, Feb. 21, 2013, http://articles.courant.com/2013-02-21/community/hc-wethersfield-bus-cameras-20130221_1_school-buses-bus-passers-bus-drivers.

[167] *See, e.g.*, Kauffman, *supra* note 9.

[168] *See, e.g.*, Jeffrey Rosen, Op-Ed, *Protect Our Right to Anonymity*, N.Y. Times, Sept. 12, 2011, http://www.nytimes.com/2011/09/13/opinion/protect-our-right-to-anonymity.html?_r=0; N.Y. Civil Liberties Union, *supra* note 8; *First 'Intelligent Security Cameras' with Facial Recognition Available in North America from Gadspot*, *supra* note 8.

[169] Somini Sengupta, *Rise of Drones in U.S. Drives Efforts to Limit Police Use*, N.Y. Times, Feb. 15, 2013, http://www.nytimes.com/2013/02/16/technology/rise-of-drones-in-us-spurs-efforts-to-limit-uses.html?hp&_r=0; Ben Wolfgang, *FAA Chief Says Drones Will Force Change at Agency*, Wash. Times, Aug. 7, 2012, http://www.washingtontimes.com/news/2012/aug/7/faa-chief-says-drones-will-force-change-at-agency/. The FAA is acting under a new federal law, the FAA Modernization and Reform Act of 2012, Pub. L. No.112-95, 126 Stat. 11 (2012).

[170] *See, e.g.*, *Jones*, 132 S. Ct. at 963 (Alito, J., concurring); United States v. Pineda-Moreno, 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc), *original opinion vacated*, 132 S. Ct. 1533 (2012).

[171] *See, e.g.*, United States v. Skinner, 690 F.3d 772 (6th Cir. 2012), *petition for cert. filed* (U.S. Dec. 26, 2012).

[172] *See, e.g.*, *Jones*, 132 S. Ct. at 963 (Alito, J., concurring).

[173] Christopher Caldwell, *A Pass on Privacy?*, N.Y. Times Mag., July 17, 2005, http://www.nytimes.com/2005/07/17/magazine/17WWLN.html?_r=0.

[174] Somini Sengupta, *Facebook Can ID Faces, but Using Them Grows Tricky*, N.Y. Times, Sept. 21, 2012, http://www.nytimes.com/2012/09/22/technology/facebook-backs-down-on-face-recognition-in-europe.html.

[175] *See, e.g.*, Am. Civil Liberties Union of Illinois v. Alvarez, 679 F.3d 583, 601 (7th Cir. 2012); Glik v. Cunniffe, 655 F.3d 78, 83 (1st Cir. 2011); Smith v. City of Cumming, 212 F.3d 1332, 1333 (11th Cir. 2000).

[176] *Cf., e.g.*, Handschu v. Special Servs. Div., 273 F. Supp. 2d 327 (S.D.N.Y. 2003).

[177] *Cf. Kyllo*, 533 U.S. at 31-33; *Ciraolo*, 476 U.S. at 213; *Brown*, 460 U.S. at 740.

[178] *Turner*, 884 A.2d at 11; *Fiorillo*, 2004 WL 1153678, at *1-5; *see also Vazquez*, 31 F. Supp. 2d at 90-91.

[179] *Jones*, 132 S. Ct. at 954-57 (Sotomayor, J., concurring); *id.* at 957-64 (Alito, J., concurring).

[180] *Cf.* Solove, *Fourth Amendment Codification*, *supra* note 148, at 754; Kerr, *supra* note 15, at 850-51.

[181] *See, e.g.*, N.Y. Civil Liberties Union, *supra* note 8; Cara Branigan, *Cell Phones Have the potential to Violate Privacy in School*, *reprinted in* Are Privacy Rights Being Violated?, *supra* note 8, at 10-16.

[182] *See, e.g.*, Rathsack, *supra* note 8.

[183] N.Y. Civil Liberties Union, *supra* note 8, at 12; Tuan Mai, *High Tech Fingerprint Scanner Scans From 20ft Away*, Tom's Guide (June 23, 2012, 9:00 PM), http://www.tomsguide.com/us/Fingerprint-Scanner-idair-airprint-security,news-15643.html; *see also* Clay Dillow, *A Fingerprint Scanner That Can Capture Prints from 20 Feet Away*, Popular Sci. (June 25, 2012, 2:18 PM), http://www.popsci.com/technology/article/2012-06/fingerprint-scanner-captures-prints-20-feet-away. Technology being developed for airports will be able to scan your heart rate from a distance, without your knowledge. Pam Benson, *Will Airports Screen for Body Signals? Researchers Hope So*, CNN (Oct. 6, 2009, 9:15 PM), http://www.cnn.com/2009/TECH/10/06/security.screening/.

[184] Conn. Gen. Stat. § 53a-189a (2013). Bills have been introduced to add language about trespasses and voyeurism involving children, H.B. 6570 and S.B. 871. Conn. Gen. Assembly, Off. Legis. Res., http://cga.ct.gov/olr/default.asp (last visited Mar. 25, 2013). Dissemination of voyeuristic materials without the consent of the person depicted is a crime, also. Conn. Gen. Stat. § 53a-189b (2013).

[185] Conn. Gen. Stat. § 53-41a (2013).

[186] § 53a-189a. There's a statute that forbids first responders from taking unauthorized pictures of crime or accident victims and imposes criminal penalties. Conn. Gen. Stat. § 53-341c (2013).

[187] *E.g.*, Conn. Gen. Stat. § 53-451 (2013).

[188] *E.g.*, Conn. Gen. Stat. § 53a-181d (2013).

[189] 3 Restatement (Second) Torts § 652B, *quoted in Gallagher*, 1997 WL 240907, at *2.

[190] § 53a-189a; *see also* John Pirro, *Prosecutor Fired for Filming Women's Legs*, newstimes.com (Aug. 7, 2012, 11:10 PM), http://www.newstimes.com/policereports/article/Prosecutor-fired-for-filming-women-s-legs-3769487.php (describing the recent case of a Connecticut prosecutor who was fired for filming women but wasn't prosecuted). There's also a federal anti-voyeurism statute aimed at taking pictures up skirts. But it applies only to federal lands and buildings and to federal maritime jurisdiction. 18 U.S.C. § 1801 (2006 & Supp. V 2011).

[191] *Cf. Kyllo*, 533 U.S. at 31-33.

[192] *Ciraolo*, 476 U.S. at 213; *see also Riley*, 488 U.S. 445 (plurality).

[193] United States v. Biasucci, 786 F.2d 504, 508-12 (2d Cir. 1986); United States v. Torres, 751 F.2d 875, 883 (7th Cir. 1984).

[194] *Kyllo*, 533 U.S. at 31-33.

[195] *Jardines*, 2013 WL 1196577, at *6. Another drug-sniffing dog case has just been decided by the Court, holding that a trained drug-sniffing dog's reaction amounts to probable cause to search a vehicle. Florida v. Harris, No. 11-817, 2013 WL 598440 (U.S. Feb. 19, 2013).

[196] Dow Chemical Co. v. United States, 476 U.S. 227, 238 & n.5 (1986).

[197] *Id.*

[198] N.Y. Civil Liberties Union, *supra* note 8, at 12.

[199] *See* Marisa L. Porges, Op-Ed., *Dead Men Share No Secrets*, N.Y. Times, Sept. 24, 2012, http://www.nytimes.com/2012/09/25/opinion/dont-kill-every-terrorist.html?_r=0.

[200] *See* Wolfgang, *supra* note 169.

[201] *See* Sengupta, *supra* note 169; Joan Lowy, *A Third of Public Fears Police Use of Drones*, Big Story, AP (Sep. 27, 2012, 3:27 PM), http://bigstory.ap.org/article/third-public-fears-police-use-drones. Nobody knows how many licenses have issued. Jennifer Lynch, *Just How Many Drone Licenses Has the FAA Really Issued?*, Electronic Frontier Found. (Mar. 1, 2013), https://www.eff.org/deeplinks/2013/02/just-how-many-drone-licenses-has-faa-really-issued.

The Senate has held hearings on the need to plug holes in privacy laws regarding drones. Matthew L. Wald, *Current Laws May Offer Little Shield Against Drones, Senators Are Told*, N.Y. Times, Mar. 20, 2013, http://www.nytimes.com/2013/03/21/us/politics/senate-panel-weighs-privacy-concerns-over-use-of-drones.html?src=rechp&_r=0. Bills have been introduced in Congress to regulate drones. *Bill Summary and Status 113th Congress (2013-14) H.R. 637, H.R. 972, H.R. 1083, H.R. 1242, S. 505*, Thomas (Library of Congress), http://www.thomas.gov/home/bills_res.html (last visited Mar. 21, 2013). *See generally* Congress-Summary.com, http://www.congress-summary.com/Home.html (last visited Mar. 19, 2013) (providing helpful search tool).

[202] Cora Currier, *Everything You Ever Wanted to Know About Drones*, ProPublica (May 31, 2012, 9:39 AM), http://www.propublica.org/article/everything-you-ever-wanted-to-know-about-drones; Jack M. Beard, *Law and War in the Virtual Era*, 103 Am. J. Int'l L. 409 (July 2009) (exploring capabilities of drones already used).

[203] Int'l Ass'n of Chiefs of Police, Aviation Comm., Recommended Guidelines for the Use of Unmanned Aircraft, Int'l Ass'n of Chiefs of Police (Aug. 2012), http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf.

[204] *See* Jeffrey Rosen, Op-Ed, *Protect Our Right to Anonymity*, N.Y. Times, Sept. 12, 2011, http://www.nytimes.com/2011/09/13/opinion/protect-our-right-to-anonymity.html?_r=0; N.Y. Civil Liberties Union, *supra* note 8; *First 'Intelligent Security Cameras'*

with Facial Recognition Available in North America from Gadspot, *supra* note 8; Thompson, *supra* note 8.

[205] Sara Reardon, *FBI Launches $1 Billion Face Recognition Project*, New Scientist, Sept. 7, 2012, http://www.newscientist.com/article/mg21528804.200-fbi-launches-1-billion-face-recognition-project.html; Sengupta, *supra* note 174.

[206] Kauffman, *supra* note 9.

[207] *Id.*

[208] *Senate Bill 41*, N.H. Gen. Ct., http://www.gencourt.state.nh.us/legislation/2007/sb0041.html (last visited Feb. 23, 2013).

[209] *See Automatic License Plate Readers: A Threat to Americans' Privacy*, Am. Civ. Liberties Union (July 30, 2012), http://www.aclu.org/automatic-license-plate-readers-threat-americans-privacy.

[210] *See Pineda-Moreno*, 617 F.3d at 1125 (Kozinski, C.J., dissenting from denial of rehearing en banc). The Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286, mandated that carriers provide location services so cell phone users could call 911.

[211] *Skinner*, 690 F.3d at 776; U.S. Cellular Corp. v. F.C.C., 254 F.3d 78, 81 (D.C. Cir. 2001).

[212] Peter Maass & Megha Rajagopalan, News Analysis, Sunday Review, *That's No Phone. That's My Tracker*, N.Y. Times, July 13, 2012, http://www.nytimes.com/2012/07/15/sunday-review/thats-not-my-phone-its-my-tracker.html.

[213] *Skinner*, 690 F.3d at 776 (internal quotation marks omitted).

[214] Maass & Rajagopalan, *supra* note 212.

[215] *See, e.g.*, Hillman & O'Rourke, *supra* note 154, at 103.

[216] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986); Conn. Gen. Stat. §§ 53-451—53-454 (2013).

[217] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986); §§ 53-451—53-454. Section 202 of the Telecommunications Act of 1996 forbids carriers from disclosing location data without consent and might apply to mobile

phones, and there are also voluntary industry regulations that provide some help. Michael G. Rhodes & Charles A. Schwab, *Mobile Commerce: A Moving Target for Legal Compliance*, Aspatore, 2012 WL 2244516, at *6-7, *9 (July 2012). The Telephone Records and Privacy Protection Act makes it illegal to obtain phone records by fraud. 18 U.S.C. § 1039 (2006 & Supp. V 2011).

[218] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

[219] *See generally In re* Application of the United States, 620 F.3d 304, 310 n.6 (3d Cir. 2010); United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012) (discussing split of authority). Bills have been introduced to amend this law regarding release of location data. *Bill Summary and Status 113th Congress (2013-14) H.R. 983, H.R. 1312, S. 639*, Thomas (Library of Congress), http://www.thomas.gov/home/bills_res.html (last visited Mar. 26, 2013).

[220] 18 U.S.C. § 2703(d) (2006 & Supp. V 2011).

[221] 18 U.S.C. § 2702(b)(8), (c)(4) (2006 & Supp. V 2011); *see also In re* Application of United States for a *Nunc Pro Tunc* Order For Disclosure of Telecomm. Records, 352 F. Supp. 2d 45, 47 (D. Mass. 2005) (citing provision); State v. Reynolds, No. CR09239695, 52 Conn. L. Rptr. 65, 2011 WL 2536472, at *2-6 (Conn. Super. Ct. June 01, 2011) (discussing provision).

[222] Conn. Gen. Stat. § 54-47aa(b), (c) (2013).

[223] *See Reynolds*, 2011 WL 2536472, at *2-7.

[224] *See* Sasso, *supra* note 10.

[225] *Id.*

[226] *See, e.g.*, *Skinner*, 690 F.3d at 777-81.

[227] *See id.* (citing *Knotts*, 460 U.S. at 281-85).

[228] *See id.*

[229] United States v. Marquez, 605 F.3d 604, 609-10 (8th Cir. 2010) (citing United States v. Karo, 468 U.S. 705, 716 (1984)).

[230] *Id.*

[231] United States v. Maynard, 615 F.3d 544, 558-68 (D.C. Cir. 2010), *aff'd on other grounds sub nom. Jones*, 132 S. Ct. 945. The *Knotts* Court responded to arguments about possible twenty-four-hour surveillance by writing: "if such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." 460 U.S. at 283-84 (citation omitted).

[232] *In re* United States for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011).

[233] *Jones*, 132 S. Ct. at 948.

[234] *Id.* at 948; *id.* at 964 n. 11 (Alito, J. concurring).

[235] *Id.* at 949-53 (majority opinion).

[236] *Id.* at 951-52.

[237] *Id.* at 957-64 (Alito, J., concurring).

[238] *Id.* at 957-62.

[239] *Id.* at 961.

[240] *Id.* at 961-62.

[241] *Cf. id.* at 958, 962.

[242] *Id.* at 963-64.

[243] *Cf. id.*

[244] *Id.*

[245] *Id.* at 954 (majority opinion); *id.* at 964 (Alito, J., concurring).

[246] *Id.* at 963-64 (Alito, J., concurring) (citing Kerr, *supra* note 15, at 805-06).

[247] *Id.* at 963-64 & n.7 (citing 18 U.S.C. §§ 2510–2522 (2006 & Supp. V) and Kerr, *supra* note 15).

[248] *Id.* at 954-57 (Sotomayor, J., concurring).

[249] *Id.* at 955-56.

[250] *Id.* at 956-57 & n.* (citing Smith v. Maryland, 442 U.S. 735 (1979), *superseded by statute*, 18 U.S.C. §§ 3121-3127 (2006), and *Miller*, 425 U.S. at 443).

[251] *Miller*, 425 U.S. at 443, *superseded by statute*, 12 U.S.C. § 3401 (2006), *as recognized in Chao*, 474 F.3d at 83.

[252] *See* RFID Technology 1-9 (Roman Espejo ed., 2009); Nancy Friedrich, *RFID Innovations Deepen Market Penetration*, Microwaves & RF (July 2007), *reprinted in* RFID Technology, *supra*, at 10-16; Annalee Newitz, *The RFID Hacking Underground*, 15 Wired, *reprinted in* RFID Technology, *supra*, at 17-27; Am. Civil Liberties Union et al., *RFID Technology May Threaten Privacy and Civil Liberties*, PrivacyRights.org (Nov. 11, 2003), *reprinted* in RFID Technology, *supra*, at 33-47; Donald Davis, *E-Passports Debut, and Not Everyone is Cheering*, 10 Card Tech. 14 (Sept. 2005), *reprinted* in RFID Technology, *supra*, at 64-76; Kenneth R. Foster & Jan Jaeger, *RFID Inside*, IEEE Spectrum (Mar. 2007), *reprinted in* RFID Technology, *supra*, at 83-93.

[253] Newitz, *supra* note 252, at 21-22.

[254] *Cf. Jones*, 132 S. Ct. at 964 (Alito, J., concurring); *Pineda-Moreno*, 617 F.3d at 1125 (Kozinski, C.J., dissenting from denial of rehearing en banc).

[255] We are grateful to the national American Civil Liberties Union and The Electronic Frontier Foundation, whose work helped us to identify these policy concerns.

[256] Michael M. Grynbaum et al., *Police Seek Man Taped Near Times Sq. Bomb Scene*, N.Y. Times, May 2, 2010, http://www.nytimes.com/2010/05/03/nyregion/03timessquare.html?pagewanted=all; Mark Mazzetti et al., *Suspect, Charged, Said to Admit to Role in Plot*, N.Y. Times, May 4, 2010, http://www.nytimes.com/2010/05/05/nyregion/05bomb.html?pagewanted=all; Benjamin Weiser & Colin Moynihan, *Guilty Plea in Times Square Bomb Plot*, N.Y. Times, June 21, 2010, http://www.nytimes.com/2010/06/22/nyregion/22terror.html.

[257] Jennifer 8. Lee, *Study Questions Whether Cameras Cut Crime*, City Room, N.Y. Times (March 3, 2009, 10:16 AM), http://cityroom.blogs.nytimes.com/2009/03/03/study-questions-whether-cameras-cut-crime/. (Her name really is "Jennifer 8. Lee.")

[258] Mark Hughes, *CCTV in the Spotlight: One Crime Solved for Every 1,000 Cameras*, Indep., Aug. 25, 2009, http://www.independent.co.uk/news/uk/crime/cctv-in-the-spotlight-one-crime-solved-for-every-1000-cameras-1776774.html.

[259] *FAQs about Camera Surveillance*, Surveillance Stud. Ctr. (Feb. 23, 2013), http://www.sscqueens.org/projects/scan_faqs.

[260] *Id.*; Jeffrey Rosen, *A Cautionary Tale for a New Age of Surveillance*, N.Y. Times, Oct. 7, 2001, http://www.nytimes.com/2001/10/07/magazine/07SURVEILLANCE.html?pagewanted=print.

[261] Jacob Sullum, *Are You Camera Ready? Police Surveillance in the Nation's Capital*, Creators Syndicate Inc., Feb. 15, 2002, www.ratical.org/ratville/CAH/linkscopy/cameraready.html.

[262] *Cf.* Alex Kozinski, *The Dead Past*, 64 Stan. L. Rev. Online 117 (2012), http://www.stanfordlawreview.org/online/privacy-paradox/dead-past (explaining that he felt his privacy invaded while watching Jerry Springer).

[263] *Cf.* Scott Shane & Sheryl Gay Stolberg, *A Brilliant Career with a Meteoric Rise and an Abrupt Fall*, N.Y. Times, Nov. 10, 2012, http://www.nytimes.com/2012/11/11/us/david-petraeus-seen-as-an-invincible-cia-director-self-destructs.html?pagewanted=1&ref=davidhpetraeus.

[264] Olmstead v. United States, 277 U.S. 438 (1928), *overruled by Katz*, 389 U.S. at 352-53, and Berger v. New York, 388 U.S. 41, 50-51 (1967).

[265] *Id.* at 456-57.

[266] *Id.* at 471-84 (Brandeis, J., dissenting).

[267] *See Katz*, 389 U.S. at 351-59.

[268] *Id.* at 351; *see also* Alderman & Kennedy, *supra* note 4, at 23 (quoting *Katz*).

[269] *Id.* at 360-61 (Harlan, J., concurring).

[270] *Id.* at 348 (majority opinion).

[271] *Cf. Berger*, 388 U.S. at 46-47 (explaining the difference between bugging and wiretapping).

[272] United States v. White, 401 U.S. 745, 746-54 (1971) (plurality); United States v. Caceres, 440 U.S. 741 (1979) (discussing *White*).

[273] *Smith*, 442 U.S. at 742.

[274] 18 U.S.C. §§ 3121-3127 (2006 & Supp. V 2011).

[275] United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008).

[276] United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001).

[277] Price v. Turner, 260 F.3d 1144, 1148-49 (9th Cir. 2001); United States v. Smith, 978 F.2d 171, 179 (5th Cir. 1992).

[278] *Price*, 260 F.3d at 1147.

[279] *Berger*, 388 U.S. at 54; *accord* Kerr, *supra* note 15, at 848 (quoting and explaining *Berger*).

[280] *Berger*, 388 U.S. at 58-60; *see also* Kerr, *supra* note 15, at 848 (elucidating case).

[281] *Berger*, 388 U.S. at 59; *see also* Kerr, *supra* note 15, at 848 (clarifying case).

[282] *Berger*, 388 U.S. at 60; *see also* Kerr, *supra* note 15, at 848 (spelling out standard).

[283] *Berger*, 388 U.S. at 60; *see also* Kerr, *supra* note 15, at 848 (listing elements).

[284] *Berger*, 388 U.S. at 58-59; *e.g.*, *Biasucci*, 786 F.2d at 508-12.

[285] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all; Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 San Diego L. Rev. 745, 745 (2007) (crediting Risen and Lichtblau with scoop); Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. Chi. L. Rev. 343 (2008) (discussing program).

[286] *See* Risen & Lichtblau, *supra* note 285.

[287] Memorandum from the U.S. Dep't of Justice on Legal Auths. Supporting the Activities of the Nat'l Sec. Agency Described by the President 2, 8-17 (Jan. 19, 2006), *available at* http://www.justice.gov/opa/whitepaperonnsalegalauthorities.pdf.

[288] *Id.* at 8 (citing United States v. United States District Court (Keith), 407 U.S. 297, 308-09 (1972)); *see also In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012-13 (FISA Ct. Rev. 2008) (upholding certain warrantless surveillance).

[289] Memorandum from the U.S. Dep't of Justice, *supra* note 287, at 2, 8-17; *see also* Anthony M. Shults, Note, *The "Surveil or Kill" Dilemma: Separation of Powers and the FISA Amendments Act's Warrant Requirement for Surveillance of U.S. Citizens Abroad*, 86 N.Y.U. L. Rev. 1590 (Nov. 2011).

That authorization says, in relevant part:

> That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224, 224 (2001).

[290] Kali Borkoski, *Suing over Surveillance Secrets*, SCOTUSblog (Oct. 29, 2012, 9:33 AM), http://www.scotusblog.com/2012/10/suing-over-surveillance-secrets/.

[291] Shane Harris, Op-Ed., *Giving In to the Surveillance State*, N.Y. Times, Aug. 22, 2012, http://www.nytimes.com/2012/08/23/opinion/whos-watching-the-nsa-watchers.html.

[292] *Id.* Provisions pending in Congress on cybersecurity would allow companies to share private data with the NSA with impunity. Adi Kamdar, *Stop CISPA: A Week of Action to Oppose Broad Cybersecurity Legislation*, Electronic Frontier Found. (Mar.

18, 2013), https://www.eff.org/deeplinks/2013/03/week-action-opposing-cispa; *Bill Summary and Status 113th Congress (2013-14) H.R. 624*, THOMAS (LIBRARY OF CONGRESS), http://www.thomas.gov/home/bills_res.html (last visited Mar. 21, 2013). This bill has just passed the House. Dave Maass & Mark M. Jaycox, *U.S. House of Representatives Shamefully Passes CISPA; Internet Freedom Advocates Prepare for Battle in the Senate*, ELECTRONIC FRONTIER FOUND. (Apr. 18, 2013), https://www.eff.org/deeplinks/2013/04/us-house-representatives-shamefully-passes-cispa-internet-freedom-advocates.

[293] Harris, *supra* note 291.

[294] Am. Civil Liberties Union v. Nat'l Sec. Agency, 493 F.3d 644 (6th Cir. 2007).

[295] Clapper v. Amnesty Int'l USA, No. 11–1025, 2013 WL 673253 (U.S. Feb. 26, 2013); *see also* Al-Haramain Islamic Found. v. Obama, Nos. 11–15468, 11–15535, 2012 WL 6582334 (9th Cir. Dec 05, 2012) (holding that FISA does not waive sovereign immunity).

[296] *See, e.g.*, RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY (2006).

[297] *See id.*

[298] 18 U.S.C. §§ 3121-3127 (2006 & Supp. V 2011).

[299] *Smith*, 442 U.S. at 742. *But see In re* U.S. for Orders (1) Authorizing Use of Pen Registers and Trap and Trace Devices, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) (holding that using PEN registers to read numbers dialed after a call is placed implicates Fourth Amendment and requires higher standard than the statute provides).

[300] 18 U.S.C. § 3121.

[301] Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522 (2006 & Supp. V 2011)).

[302] *See* 18 U.S.C. § 2511 (2006 & Supp. V 2011); Solove, Fourth Amendment Codification, supra note 148, at 776; cf. Bartnicki v. Vopper, 532 U.S. 514, 523-24 (2001).

[303] *See, e.g.*, Solove, *Fourth Amendment Codification*, *supra* note 148, at 754; Kerr, supra note 15, at 850-51.

[304] *See, e.g.*, Kerr, *supra* note 15, at 851; Solove, *Fourth Amendment Codification*, *supra* note 148, at 761.

[305] 18 U.S.C. § 2518(8)(d) (2006 & Supp. V 2011); United States v. Principie, 531 F.2d 1132, 1142 (2d Cir. 1976); Kerr, *supra* note 15, at 852.

[306] 18 U.S.C. § 2515 (2006 & Supp. V 2011).

[307] 18 U.S.C. § 2511; *Bartnicki*, 532 U.S. at 517-35 (holding law unconstitutional as applied to radio commentator who broadcast illegally obtained recording, but did nothing wrong in acquiring it).

[308] 18 U.S.C. § 2520 (2006 & Supp. V 2011).

[309] 18 U.S.C. § 2511(2)(c), (d).

[310] *Id.*

[311] *Bartnicki*, 532 U.S. at 517-35.

[312] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[313] 18 U.S.C. § 2511(1)(a); Kerr, *supra* note 15, at 851.

[314] *Bartnicki*, 532 U.S. at 524.

[315] 18 U.S.C. § 2701(a), (b) (2006 & Supp. V 2011). Civil remedies are available, also. 18 U.S.C. § 2707 (2006 & Supp. 2011).

[316] 18 U.S.C. §§ 2511, 2701, 2702 (2006 & Supp. V 2011).

[317] Communications Assistance for Law Enforcement Act, Pub. L. No. 103–414, 108 Stat. 4279 (1994); *see also Bartnicki*, 532 U.S. at 524; Charles J. Sykes, The End of Privacy 163-66 (1999) (describing CALEA). The Electronic Communications Privacy Act had expressly excluded the radio part of cordless phones from the definition of both wire and electronic communications, but CALEA deleted those exclusions.

[318] *See, e.g.*, Mani Potnuru, *Limits on the Federal Wiretap Act's Ability to Protect Against Wi-Fi Sniffing*, 111 MICH. L. REV. 89, 103 (2012).

[319] Solove, *Fourth Amendment Codification*, *supra* note 148, at 761.

[320] 18 U.S.C. § 2703(a) (2006 & Supp. V 2011).

[321] 18 U.S.C. § 2703(d). The Sixth Circuit has held this provision fails to provide a constitutional level of protection to emails. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010); *see also* Hanni Fakhoury et al., *When Will Our Email Betray Us? An Email Privacy Primer in Light of the Petraeus Saga*, ELECTRONIC FRONTIER FOUND. (Nov. 14, 2012), https://www.eff.org/deeplinks/2012/11/when-will-our-email-betray-us-email-privacy-primer-light-petraeus-saga (describing law). For its part, the government takes the view that many emails may be accessed without a warrant even if they're newer than 180 days. Fakhoury, *supra*. A federal appellate court has rejected the government's position. Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

Congress has convened hearings on amending the law to protect emails older than 180 days. Mark M. Jaycox, *Reform to Update Online Privacy Law Continues to Move Forward: Today, a Hearing in the House and Movement in the Senate*, ELECTRONIC FRONTIER FOUND. (Mar. 19, 2013), https://www.eff.org/deeplinks/2013/03/ecpa-reform-continues-move-forward-today-hearing-house-and-movement-senate. And bills have been introduced. *Bill Summary and Status 113th Congress (2013-14) H.R. 983, S. 607*, THOMAS (LIBRARY OF CONGRESS), http://www.thomas.gov/home/bills_res.html (last visited Mar. 19, 2013). The Senate bill to protect all emails has just passed out of the Judiciary Committee. Somini Sengupta, *Updating an E-Mail Law from the Last Century*, N.Y. TIMES, Apr. 24, 2013, http://www.nytimes.com/2013/04/25/technology/updating-an-e-mail-law-from-the-last-century.html?ref=email&_r=0.

[322] 18 U.S.C. §§ 2703(b), 2705 (2006 & Supp. V 2011).

[323] 18 U.S.C. § 2703(c). Under the language of the statute, cell-location information requires notice and at least a court order, but

some more basic customer information does not. *In re* Application of the United States, 620 F.3d 304 (3d Cir. 2010).

[324] 18 U.S.C. § 2702(b)(7)(A)(ii), (b)(8), (c)(4) (2006 & Supp. V 2011); *see also Reynolds*, 52 Conn. L. Rptr. 65, 2011 WL 2536472, at *2-6 (discussing provision).

[325] *See* Sasso, *supra* note 10.

[326] 18 U.S.C. § 2515 (2006 & Supp. V 2011); *see also* Derek T. Fettig, *When "Good Faith" Makes Good Sense: Applying Leon's Exception to the Exclusionary Rule to the Government's Reasonable Reliance on Title III Wiretap Orders*, 49 Harv. J. on Legis. 373, 380 (2012) (noting that section 2515 provides for suppression of wire and oral communications, but not electronic communications like email).

[327] Reuters, *Bush Family E-Mail Accounts Are Hacked*, N.Y. Times, Feb. 8, 2013, http://www.nytimes.com/2013/02/09/us/bush-family-e-mail-accounts-are-hacked.html.

[328] Shane & Stolberg, supra note 263; John H. Cushman, Jr., *Woman in Petraeus Case Won't Be Charged with Cyberstalking*, N.Y. Times, Dec. 18, 2012, http://www.nytimes.com/2012/12/19/us/woman-in-petraeus-case-wont-be-charged-with-cyberstalking.html?ref=davidhpetraeus.

[329] *Cf.* Michael R. Gordon, *A Retiring General Notes 'the Price We Have Paid'*, N.Y. Times, Feb. 21, 2013, http://www.nytimes.com/2013/02/22/world/asia/general-allen-gives-farewell-talk.html.

[330] *Keith*, 407 U.S. at 308-09.

[331] Shults, *supra* note 289, at 1595.

[332] Foreign Intelligence Surveillance Act of 1978, Pub L. No. 95-511, 92 Stat. 1783 (1978).

[333] Matthew A. Anzaldi & Jonathan W. Gannon, *In Re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act: Judicial Recognition of Certain Warrantless Foreign Intelligence Surveillance*, 88 Tex. L. Rev 1599, 1605 (2010); Shults, *supra* note 289, at 1597-98.

[334] Shults, *supra* note 289, at 1597-98.

[335] *Id.*

[336] Amnesty Int'l USA v. Clapper, 638 F.3d 118, 123-24 (2d Cir. 2011), *rev'd*, 2013 WL 673253; Shults, *supra* note 289, at 1598.

[337] Shults, *supra* note 289, at 1599.

[338] Daniel E. Lungren, *A Congressional Perspective on The Patriot Act Extenders*, 26 Notre Dame J.L. Ethics & Pub. Pol'y 427, 429-35 (2012) (citing Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT ACT), Pub. L. No. 107-56, 115 Stat. 272 (2001) and Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004)).

[339] Lundgren, *supra* note 338, at 430-51.

[340] *Id.* at 436-42.

[341] *Id.* at 443-50; John Doe, Inc. v. Mukasey, 549 F.3d 861, 862 (2d Cir. 2008); *In re* National Sec. Letter, No. C 11–02173 SI, 2013 WL 1095417 (N.D. Cal. Mar. 14, 2013).

[342] Shults, *supra* note 289, at 1599. The law is 50 U.S.C.A. § 1881a (2013).

[343] *Amnesty Int'l* USA, 2013 WL 673253, at *4.

[344] *Id.*

[345] 50 U.S.C. § 1881a; *Amnesty Int'l* USA, 2013 WL 673253, at *4.

[346] Editorial, *Surveillance and Accountability*, N.Y. Times, Oct. 28, 2012, http://www.nytimes.com/2012/10/29/opinion/surveillance-and-accountability.html.

[347] FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (2012).

[348] United States v. D'Antoni, 874 F.2d 1214, 1218-19 (7th Cir. 1989). State law may be relevant to a federal prosecution when evidence was originally obtained pursuant to warrants issued by state authorities under state standards; in such a case the warrants' validity is a question of state law. *See, e.g.*, *Manfredi*, 488 F.2d at 598.

[349] State v. Boyd, 992 A.2d 1071, 1079-83 (Conn. 2010).

[350] State v. Gonzalez, 898 A.2d 149, 155-57 (Conn. 2006); State v. Grullon, 562 A.2d 481 (Conn. 1989); State v. DelVecchio, 464 A.2d 813 (Conn. 1983).

[351] CONN. GEN. STAT. §§ 54-41a—54-41u (2013). Nothing in the law requires an officer to get a warrant when he's one of the people on the call and consents to the eavesdropping. *Grullon*, 562 A.2d 481.

[352] *See McVeigh*, 620 A.2d at 138-39 & n.17.

[353] *See id.* at 148.

[354] *Bartnicki*, 532 U.S. at 524.

[355] *See, e.g.*, State v. Vincente, 688 A.2d 359 (Conn. App. Ct. 1997).

[356] *McVeigh*, 620 A.2d at 138-39. For example, the state's wiretap statute requires authorities to follow the *Aguilar-Spinelli* test, which is a more restrictive standard for probable-cause warrants than the federal law requires. State v. Telesca, 508 A.2d 1367, 1373 (Conn. 1986); State v. Levine, 497 A.2d 774, 776 (Conn. App. Ct. 1985).

[357] Conn. Gen. Stat. § 54-41h (2013).

[358] Conn. Gen. Stat. §§ 54-41i, 54-41p, 54-41r, 54-41t (2013). Section 54-41r is the one that creates a civil cause of action for victims of the criminal wiretapping statute.

[359] Conn. Gen. Stat. §§ 54-41m, 54-41u (2013). Conn. Gen. Assembly, Office of Legislative Research, Summary of 2002 Public Acts 141 (undated), *available at* http://cga.ct.gov/olr/Documents/year/PASUMBK/2002PASUMBK-20021216_Summary%20of%202002%20Public%20Acts.pdf. Another statute reads: "No evidence obtained illegally by the use of any electronic device is admissible in any court of this state." Conn. Gen. Stat. § 52-184a (2013).

[360] Conn. Gen. Stat. § 54-47aa(a)-(c) (2013).

[361] § 54-47aa(d).

[362] § 54-47aa(g).

[363] *See Reynolds*, 2011 WL 2536472, at *2-7.

[364] Majority and Minority Staff of S. Permanent Subcomm. on Investigations, Comm. on Homeland Sec. & Gov't Affairs, 112th Cong., Rep. on Federal Support for and Involvement in State and Local Fusion Centers 1-13 (2012), *available at* http://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers.

[365] *Id.* at 6-7.

[366] *Id.*

[367] *Id.* at 2-4.

[368] *Id.*

[369] *Id.* A bill to bolster Fusion Centers' security efforts focused on urban mass transit has been introduced. *Bill Summary and Status 113th Congress (2013-14) H.R. 1210*, Thomas (Library of Congress), http://www.thomas.gov/home/bills_res.html (last visited Mar. 21, 2013). *See generally* Congress-Summary.com, http://www.congress-summary.com/Home.html (last visited Mar. 19, 2013) (providing helpful search tool).

[370] Conn. Gen. Stat. § 53a-187, 53a-189 (2013); *see also* State v. McLoughlin, 723 A.2d 827, 508 (Conn. Super. Ct. 1998) (holding that cordless calls are covered, too). Wiretapping doesn't include a telephone company's normal use or operation of facilities. § 53a-187.

[371] Conn. Gen. Stat. § 53a-187(b).

[372] Conn. Gen. Stat. § 53a-188 (2013).

[373] Conn. Gen. Stat. § 53-422 (2013).

[374] Conn. Gen. Stat. § 52-570d (2013). Whether this statute might apply to interstate calls is unclear and may depend upon a complex choice-of-laws analysis. *See* Lord v. Lord, No. CV010380279, 33 Conn. L. Rptr. 88, 2002 WL 31125621 (Conn. Super. Ct. Aug. 20, 2002). A pending bill, S.B. 1151, would amend this section. Conn. Gen. Assembly, Off. Legis. Res., http://cga.ct.gov/olr/default.asp (last visited Apr. 2, 2013).

[375] Conn. Gen. Stat. § 52-570d (2013).

[376] *Id.*

[377] § 53-422.

[378] Conn. Gen. Stat. §§ 53-451—53-454 (2013); 18 U.S.C. § 1030 (2006 & Supp. V 2011).

[379] 18 U.S.C. § 1030(3)(2).

[380] *FTC Resources for Reporters, Making Sure Companies Keep Their Privacy Promises to Consumers*, Fed. Trade Commission, http://www.ftc.gov/opa/reporter/privacy/privacypromises.shtml (last visited Mar. 21, 2013); *see also* Dennys Marcelo Antonialli, Note, *Watch Your Virtual Steps: An Empirical Study of the Use of Online Tracking Technologies in Different Regulatory Regimes*, 8 Stanford J. of C.R. & C.L. 323, 335 & n.45 (Aug. 2012) (citing Life is Good, Inc., No. C-4218, 2008 WL 1839971 (F.T.C. Apr. 16, 2008) (consent order); Premier Capital Lending, Inc., No. C-4241, 2008 WL 5266769 (F.T.C. Dec. 10, 2008) (consent order)); *In re* Google, F.T.C. Docket No. C-4336, 2011 WL 5089551 (F.T.C. Oct. 13, 2011).

[381] *See* Sykes, *supra* note 317, at 137-51; Alderman & Kennedy, *supra* note 4, at 277-320; Jesse Leavenworth, *ACLU Says Proposed Manchester Social Media Policy Violates Free Speech*, Hartford Courant, May 25, 2012, http://articles.courant.com/2012-05-25/community/hc-manchester-school-social-media-0525-20120525_1_social-media-school-board-school-rules-and-regulations.

[382] *See* Sykes, *supra* note 317, at 137-51; Alderman & Kennedy, *supra* note 4, at 277-320.

[383] Chris Petersen, *Who's Watching You? Internet Monitoring in the Workplace Is Not Only Common, It's Necessary*, 9 U.S. Bus. Rev. 6 (2008), *reprinted* in Privacy 204 (Roman Espejo ed., 2011).

[384] 18 U.S.C. § 2510(5)(a), (2006 & Supp. V 2011).

[385] Watkins v. L.M. Berry & Co., 704 F.2d 577, 583 (11th Cir. 1983); Arias v. Mut. Cent. Alarm Serv., 202 F.3d 553, 558-60 (2d Cir. 2000).

[386] 18 U.S.C. § 2511(2)(c), (d).

[387] *E.g.*, *Watkins*, 704 F.2d at 583; *cf. Arias*, 202 F.3d at 558-59.

[388] *Id.*

[389] Conn. Gen. Stat. §§ 31-48b(a), 31-48d(a) (2013).

[390] Conn. Gen. Stat. § 31-48b(d) (2013). Also, state labor laws forbid spying on activities to organize a union. Conn. Gen. Stat. §§ 31-48b(d), 31-105 (2013). Certain surveillance of union activity is forbidden under the National Labor Relations Act, too. James R. Glenn, *Can Friendly Go Too Far? Ramifications of the NLRA on Employer Practices in a Digital World*, 2012 U. Ill. J.L. Tech. & Pol'y 219 (2012).

[391] Conn. Gen. Stat. § 31-48d(b)(1).

[392] Conn. Gen. Stat. § 31-48d(b)(2).

[393] Conn. Gen. Stat. § 31-48d(c); Gerardi v. City of Bridgeport, 985 A.2d 328, 334-35 (Conn. 2010).

[394] Conn. Gen. Stat. § 52-570d (2013).

[395] *E.g.*, *Devino*, 206 F. Supp. 2d at 309-10.

[396] *Cf.* City of Ontario v. Quon, 130 S. Ct. 2619, 2624-33 (2010).

[397] *Cf. id.*

[398] *See* Sykes, *supra* note 317, at 139-41; Alderman & Kennedy, *supra* note 4, at 310-17.

[399] 18 U.S.C. §§ 2510(5)(a), 2511(2)(a)(i) (2006 & Supp. V 2011); *see also* Hall v. Earthlink Network, Inc., 396 F.3d 500 (2d Cir. 2005).

[400] 18 U.S.C. § 2511(2)(c), (d). The Stored Communications Act, too, permits access with consent, among other exceptions. 18 U.S.C. § 2701(a)(1) (1994).

[401] Conn. Gen. Stat. § 31-48d (2013).

[402] *Quon*, 130 S. Ct. at 2624-33.

[403] Conn. Gen. Stat. §§ 31-48b(b), 31-48d(b) (2013).

[404] §§ 31-48b(b), 31-48d(b).

[405] Amy B. Crane, *Workplace Privacy? Forget It*, BANKRATE.COM, July 18, 2005, *reprinted in* ARE PRIVACY RIGHTS BEING VIOLATED?, supra note 8, at 49.

[406] § 31-48d(b).

[407] CONN. GEN. STAT. §§ 31-48b(d), 31-105 (2013).

[408] 18 U.S.C. § 2511 (2006 & Supp. V 2011); CONN. GEN. STAT. §§ 53a-187, 53a-189 (2013).

[409] 18 U.S.C. § 2511(2)(c), (d).

[410] *Cf. Gerardi*, 985 A.2d at 330-35.

[411] *Id.* A collective-bargaining agreement might forbid such monitoring.

[412] 29 U.S.C. §§ 2001-09 (2006 & Supp. V 2011); CONN. GEN. STAT. § 31-51g (2013).

[413] 42 U.S.C. §§ 12101-12213 (2006 & Supp. V 2011); 42 U.S.C. §§ 2000ff—2000ff-11 (2006 & Supp. V 2011); CONN. GEN. STAT. § 46a-60 (2013).

[414] People who write about privacy love to focus on one that Target used to give security applicants asking for responses to statements like: "I believe my sins are unpardonable. . ." or "I wish I were not bothered by thoughts about sex. . . . " *See, e.g.*, SYKES, *supra* note 317, at 145 (internal quotation marks omitted); *accord* ALDERMAN & KENNEDY, *supra* note 4, at 277-90 (discussing test).

[415] *See, e.g.*, Lewis v. City of Chicago, 130 S. Ct. 2191 (2010); Conn. Inst. for the Blind v. Comm'n on Human Rights and Opportunities, 405 A.2d 618 (Conn. 1978).

[416] CONN. GEN. STAT. § 31-51v (2013).

[417] CONN. GEN. STAT. § 31-51x(a) (2013).

[418] Poulos v. Pfizer, Inc., 711 A.2d 688, 692 (Conn. 1998).

[419] CONN. GEN. STAT. § 31-51x(b) (2013); *see* CONN. GEN. STAT. § 31-128a(2) (2013).

[420] 49 U.S.C.A. § 5331 (2013); 49 U.S.C. § 45102 (2006 & Supp. V 2011)

[421] CONN. GEN. STAT. §§ 31-51u, 31-51v, 31-51w(a) (2013).

[422] Conn. Gen. Stat. §§ 31-51z (2013). Disclosure of drug tests might also give rise to a common-law tort claim. Fallstrom v. L.K. Comstock & Co., No. CV990152583S, 2001 WL 88269 (Conn. Super. Ct. Jan. 22, 2001).

[423] Conn. Gen. Stat. §§ 31-51aa, 31-51bb (2013).

[424] Conn. Gen. Stat. § 31-51t (2013).

[425] *Quon*, 130 S. Ct. at 2624-33. There are federal laws and guidelines for testing federal employees and contractors. 41 U.S.C. §§ 8102-8106 (2006 & Supp. V 2011); 53 Fed. Reg. 11,970 (Apr. 11, 1988).

[426] Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 665 (1989).

[427] Conn. Gen. Stat. § 31-128a(4) (2013); City of Hartford v. Freedom of Info. Comm'n, 518 A.2d 49, 54 (Conn. 1986).

[428] § 31-128a(5), (6), & (7).

[429] § 31-128a(5).

[430] Conn. Gen. Stat. § 31-128f (2013).

[431] Conn. Gen. Stat. §§ 31-128b, 31-128g (2013). A pending bill, S.B. 910, would amend subsection 128b and 128e, "To provide an employee or former employee the right to copy his or her personnel files and require employers to provide copies of any documented discipline notices and copies of statements notifying an employee of the employee's rights to dispute certain documents in his or her personnel file." Conn. Gen. Assembly, Off. Legis. Res., http://cga.ct.gov/olr/default.asp (last visited Mar. 25, 2013).

[432] Conn. Gen. Stat. § 31-128e (2013).

[433] § 31-128b.

[434] § 31-128f; Conn. Gen. Stat. § 31-128c (2013).

[435] §§ 31-128c, 31-128e, 31-128g.

[436] Conn. Gen. Stat. § 31-128a(5), (7) (2013).

[437] Conn. Gen. Stat. § 31-128j (2013).

[438] § 31-128a(4); *City of Hartford*, 518 A.2d at 54.

[439] Conn. Gen. Stat. § 4-191 (1977 & West Supp. 1998) (repealed 1979), *cited in* Steven C. Carlson & Ernest D. Miller, *Public Data and Personal Privacy*, 16 Santa Clara Computer & High Tech. L.J. 83, 90 & n.26 (1999).

[440] Conn. Gen. Stat. §§ 1-200—1-259 (2013).

[441] § 1-210(b)(2). There's also a law forbidding release of some employees' addresses. Conn. Gen. Stat. § 1-217 (2013). It was amended in the state's 2012 legislative session to render release punishable only if it's done willfully and wantonly. Conn. Gen. Assembly, Office of Legislative Research, Summary of 2012 Public Acts 127-29 (undated), *available at* http://cga.ct.gov/olr/Documents/year/PASUMBK/2012PASUMBK-20120926_Summary%20of%202012%20Public%20Acts.pdf.

[442] Conn. Gen. Stat. § 1-214 (2013).

[443] *Pane*, 841 A.2d 684 at 691-92, *abrogated on other grounds by Grady*, 984 A.2d 684; *Perkins*, 635 A.2d at 789-92.

[444] Conn. Gen. Stat. § 1-206(b)(2) (2013); *Pane*, 841 A.2d 684 at 691-92.

[445] Conn. Gen. Stat. §§ 4-190—4-204 (2013).

[446] 5 U.S.C. § 552a(d) (2006 & Supp. V 2011); *Nelson*, 131 S. Ct. at 751.

[447] 5 U.S.C. § 552(b)(6) (2006 & Supp. V 2011).

[448] *Whalen*, 429 U.S. at 599-600; *Nixon*, 433 U.S. at 457-60.

[449] *See Nelson*, 131 S. Ct. at 751; *Whalen*, 429 U.S. at 599-600; *Nixon*, 433 U.S. at 457-60.

[450] *See Nelson*, 131 S. Ct. at 751-56; *Whalen*, 429 U.S. at 599-600; *Nixon*, 433 U.S. at 457-60.

[451] *See, e.g.*, Flaherty v. Seroussi, 209 F.R.D. 300, 304 (N.D.N.Y. 2002).

[452] Fed. R. Civ. P. 24(b).

[453] 50 U.S.C. §§ 1861-1862 (2006 & Supp. 2011); R. Jeffrey Smith, *Report Details Missteps in Data Collection*, Wash. Post,

Mar. 10, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/03/09/AR2007030902353.html.

[454] Steven Greenhouse, *Company Accused of Firing over Facebook Post*, N.Y. Times, Nov. 8, 2010, http://www.nytimes.com/2010/11/09/business/09facebook.html. A bill, S.B. 159, has been introduced in the General Assembly to forbid employers or potential employers from demanding passwords to personal accounts. Conn. Gen. Assembly, Off. Legis. Res., http://cga.ct.gov/olr/default.asp (last visited Mar. 25, 2013).

[455] The general rule is that public employees are protected by the First Amendment when they speak as private citizens about public things. Looney v. Black, 702 F.3d 701, 710 (2d Cir. 2012).

[456] *See, e.g.*, Craig Nydick, *The British Invasion (of Privacy): DNA Databases in the United Kingdom and United States in the Wake of the Marper Case*, 23 Emory Int'l L. Rev. 609, 621 (2009) (quoting Barry Steinhardt, Associate Director, American Civil Liberties Union); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. Rev. 1814, 1846 (2011).

[457] *See* Samuel J. Miller, *Electronic Medical Records: How the Potential for Misuse Outweighs the Benefits of Transferability*, 4 J. Health & Biomedical L. 353 (2008).

[458] *See* Ian O'Neill, *Disparate Impact, Federal/State Tension, and the Use of Credit Scores by Insurance Companies*, 19 Loy. Consumer L. Rev. 151, 152-53 (2007).

[459] Joanna Penn, Note, *Behavioral Advertising: The Cryptic Hunter and Gatherer of the Internet*, 64 Fed. Comm. L.J. 599, 601 (2012).

[460] *See id.* at 604-09; Timothy J. Shrake II, *Who's Following You: The Federal Trade Commission's Proposed "Do Not Track" Framework and Online Behavioral Advertising*, 36 S. Ill. U. L.J. 383, 383-85 (2012).

[461] *See, e.g.*, Anne Klinefelter, *When to Research is to Reveal: The Growing Threat to Attorney and Client Confidentiality from Online Tracking*, 16 Va. J.L. & Tech. 1 (2011).

[462] *See* Colin C. Richard, *Mobile Remittances and Dodd-Frank: Reviewing the Effects of the CFPB Regulations*, 12 U. Pitt. J. Tech. L. & Pol'y 1, 1-2 (2012).

[463] Facebook, http://www.facebook.com/ (last visited Feb. 23, 2013).

[464] *See* RFID Technology, *supra* note 252, at 1-9; Friedrich, *supra* note 252, at 10-16; Newitz, *supra* note 252, at 17-27; Am. Civil Liberties Union et al., *supra* note 252, at 33-47; Davis, *supra* note 252, at 64-76; Foster & Jaeger, *supra* note 252, at 83-93.

[465] *See* RFID Technology, *supra* note 252, at 1-9; Foster & Jaeger, *supra* note 252, at 83-93. In 2012 we successfully opposed Senate Bill No. 288—An Act Requiring a Study of Radio-Frequency Identification for Motor Vehicle Registration.

[466] *See, e.g.*, Schwartz & Solove, *supra* note 456, at 1846.

[467] *See* Newitz, *supra* note 252, at 17-27; Am. Civil Liberties Union et al., *supra* note 252, at 33-47; Davis, *supra* note 252, at 64-76.

[468] *See* Newitz, *supra* note 252, at 17-27; Am. Civil Liberties Union et al., *supra* note 252, at 33-47; Davis, *supra* note 252, at 64-76.

[469] David Streitfeld, *Google Concedes That Drive-by Prying Violated Privacy*, N.Y. Times, Mar. 12, 2013, http://www.nytimes.com/2013/03/13/technology/google-pays-fine-over-street-view-privacy-breach.html?hp&_r=0.

[470] *See* Sykes, *supra* note 317, at 3-12.

[471] *See* Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 Wash. U. L.Q. 461, 498 & n.98 (1999) (citations omitted).

[472] 42 U.S.C. § 405 (2006 & Supp. V 2011).

[473] *Id.* A bill has been introduced to take Social Security numbers off Medicare cards, to guard privacy. *Bill Summary and Status 113th Congress* (2013-14) H.R. 612, Thomas (Library of Congress), http://www.thomas.gov/home/bills_res.html (last visited Mar. 21, 2013). *See generally* Congress-Summary.com, http://www.congress-summary.com/Home.html (last visited Mar. 19, 2013) (providing helpful search tool).

[474] *See* Julie E. Rones, *Social Security Numbers on the Drivers License*, 9-APR NBA Nat'l B.A. Mag. 32 (1995).

[475] 5 U.S.C. § 552a(a)(4) (2006 & Supp. V 2011).

[476] 5 U.S.C. § 552a(e)(1), (d)(1)-(2), (b); *Nelson*, 131 S. Ct. at 753-54.

[477] 5 U.S.C. § 552a(e)(3). The Privacy Act of 1974 was amended by the Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507, and the Computer Matching and Privacy Protection Amendments of 1990, Pub. L. 101-508, 104 Stat. 1388, and is supplemented by the E-Government Act of 2002, Pub. L. 107-347, 116 Stat. 2899. A bill has just passed the U.S. House of Representatives to amend relevant portions of this last act. *Congress, Bills, H.R. 1163*, Govtrack.us, http://www.govtrack.us/congress/bills/113/hr1163 (last visited Apr. 28, 2013). Other statutes govern confidentiality of tax returns and information. 26 U.S.C. § 6103 (2006 & Supp. V 2011); 26 U.S.C. § 7213A (2006 & Supp. V 2011).

[478] Conn. Gen. Stat. § 4-190(9) (2013) (internal quotation marks omitted).

[479] Conn. Gen. Stat. § 4-193(c), (d), (e) (2013).

[480] *See, e.g.*, Carlson & Miller, *supra* note 439, at 91, 95, 108.

[481] Conn. Gen. Stat. § 1-210 (2013).

[482] § 1-210(b)(2); Conn. Gen. Stat. § 1-214 (2013).

[483] Conn. Gen. Stat. § 11-25 (2013).

[484] 18 U.S.C. §§ 2721-2725 (2006 & Supp. V 2011); Conn. Gen. Stat. § 14-10 (2013); Maracich v. Spears, 675 F.3d 281 (4th Cir. 2012), *cert. granted*, 133 S. Ct. 98 (2012).

[485] Carlson & Miller, *supra* note 439, at 99.

[486] Conn. Gen. Stat. §§ 45a-743—45a-757 (2013). The legislature recently amended laws regarding adoption proceedings. Conn. Gen. Assembly, Office of Legislative Research, *supra* note 441, at 21-25.

[487] *See Nelson*, 131 S. Ct. at 751; *Whalen*, 429 U.S. at 599-600; *Nixon*, 433 U.S. at 457-60.

[488] *See Nelson*, 131 S. Ct. at 751; *Nixon*, 433 U.S. at 457-60.

[489] *See Whalen*, 429 U.S. 589.

[490] 15 U.S.C. § 45 (2006 & Supp. V 2011).

[491] *See* Fed. Reserve Bd., Consumer Compliance Handbook: Federal Trade Commission Act – Section 5, at 1 (June 2008), *available at* http://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf.

[492] *FTC Resources for Reporters, Making Sure Companies Keep Their Privacy Promises to Consumers*, Fed. Trade Commission, http://www.ftc.gov/opa/reporter/privacy/privacypromises.shtml (last visited Mar. 21, 2013); *see also* Antonialli, *supra* note 380, at 335 & n.45 (Aug. 2012) (citing *Life is Good*, 2008 WL 1839971; *Premier Capital Lending*, 2008 WL 5266769); *Google*, 2011 WL 5089551.

[493] Conn. Gen. Stat. §§ 42-110a—42-110q (2013).

[494] Conn. Gen. Stat. §§ 42-470—42-479 (2013).

[495] § 42-470(a); Conn. Gen. Stat. § 42-471(c) (2013).

[496] §§ 42-470, 42-471.

[497] §§ 42-470—42-472d. There's also a statute to prohibit disclosing of your cell number without your consent. Conn. Gen. Stat. §16-247s (2013).

[498] Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999); 15 U.S.C. §§ 6801-6809 (2006 & Supp. V 2011).

[499] 15 U.S.C. § 6802(b)(1)(B) (2006 & Supp. V 2011), *cited in* Ryan L. Waggoner, Note, *Privacy of Personal Information in the Financial Services Sectors of the United States and Japan: The Gramm-Leach-Bliley Act and the Financial Services Agency Guidelines*, 4 I/S: J. L. & Pol'y for Info. Soc'y 873, 889 (Winter 2008-2009).

An amendment to Gramm-Leach-Bliley to except certain institutions that haven't changed their privacy policies from sending a new notice just passed the House by voice vote, and such a bill has been introduced in the Senate. *Bill Summary and Status 113th Congress (2013-14) H.R. 749, S. 635*, Thomas (Library

of Congress), http://www.thomas.gov/home/bills_res.html (last visited Mar. 26, 2013). *See generally* Congress-Summary.com, http://www.congress-summary.com/Home.html (last visited Mar. 19, 2013) (providing helpful search tool).

[500] 15 U.S.C. § 6821 (2006 & Supp. V 2011).

[501] 15 U.S.C. § 6802(e)(5).

[502] Right to Financial Privacy Act, Pub. L. No. 95-630, 92 Stat. 3697 (1978); 12 U.S.C. §§ 3401--3422 (2006 & Supp. V 2011).

[503] *See* S.E.C. v. Jerry T. O'Brien, Inc., 467 U.S. 735, 745-46 (1984).

[504] Conn. Gen. Stat. §§ 36a-42, 36a-43 (2013).

[505] §§ 36a-42, 36a-43.

[506] § 36a-43.

[507] Ruth Desmond, *Consumer Credit Reports and Privacy in the Employment Context: The Fair Credit Reporting Act and the Equal Employment for All Act*, 44 U.S.F. L. Rev. 907, 908 (2010).

[508] Experian, http://www.experian.com/index-bu.html (last visited Feb. 27, 2013); Equifax, http://www.equifax.com/home/en_us (last visited Feb. 27, 2013); TransUnion, http://www.transunion.com/ (last visited Feb. 27, 2013).

[509] Angela Littwin, *Coerced Debt: The Role of Consumer Credit in Domestic Violence*, 100 Cal. L. Rev. 951, 955, 1000 (2012).

[510] 15 U.S.C. §§ 1681—1681x (2006 & Supp. V 2011).

[511] Safeco Ins. Co. of Am. v. Burr, 551 U.S. 47, 52-53 (2007); TRW Inc. v. Andrews, 534 U.S. 19, 23 (2001). Pending bills would amend disclosures under the Fair Credit Reporting Act. *Bill Summary and Status 113th Congress (2013-14) H.R. 1002, S. 471*, Thomas (Library of Congress), http://www.thomas.gov/home/bills_res.html (last visited Mar. 21, 2013). See generally Congress-Summary.com, http://www.congress-summary.com/Home.html (last visited Mar. 19, 2013) (providing helpful search tool).

[512] *Safeco Ins. Co. of Am.*, 551 U.S. at 53.

[513] Longman v. Wachovia Bank, N.A., 702 F.3d 148, 150 (2d Cir. 2012).

[514] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003).

[515] Van Straaten v. Shell Oil Products Co. LLC, 678 F.3d 486, 487 (7th Cir. 2012); Long v. Tommy Hilfiger U.S.A., Inc., 671 F.3d 371, 373-74 (3d Cir. 2012); Killingsworth v. HSBC Bank Nevada, N.A., 507 F.3d 614, 618-24 (7th Cir. 2007). The Act does not permit you to sue the federal government for displaying too much credit card information on receipts. United States v. Bormes, 133 S. Ct. 12 (2012).

[516] Conn. Gen. Stat. §§ 36a-695—36a-704 (2013).

[517] 15 U.S.C. § 1681b (2006 & Supp. V 2011).

[518] 15 U.S.C. §§ 1681e (2006 & Supp. V 2011).

[519] 15 U.S.C. § 1681i (2006 & Supp. V 2011); Robinson v. Equifax Info. Servs., 560 F3d 235 (4th Cir. 2009); Conn. Gen. Stat. §§ 36a-699a, 36a-699b, 36a-699f, 36a-700 (2013).

[520] 15 U.S.C. § 1681i; §§ 36a-699a, 36a-699b, 36a-699f, 36a-700.

[521] § 36a-699b.

[522] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (1996).

[523] Health Information Technology for Economic and Clinical Health Act , Pub. L. No. 111–5, §§ 13401, 13404, 123 Stat. 115, 260, 264 (2009).

[524] 45 C.F.R. §§ 164.500—164.534 (2012 & Supp.).

[525] 45 C.F.R. § 164.508(b)(4) (2012 & Supp.).

[526] 45 C.F.R. §§ 164.522, 164.524, 164.526, 164.528 (2012 & Supp.).

[527] 42 U.S.C. §§ 17921–17953 (2006 & Supp. V 2011).

[528] Conn. Gen. Stat. § 38a-983 (2013).

[529] 45 C.F.R. § 164.512 (2012 & Supp.); 42 U.S.C. §§ 12101-12213 (2006 & Supp. V 2011).

[530] 45 C.F.R. § 164.512; State v. Russo, 790 A.2d 1132, 1150-51 (Conn. 2002).

[531] 50 U.S.C. § 1861 (2006 & Supp. V 2011).

[532] Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011).

[533] *Id.*

[534] *E.g.*, *Jaffee*, 518 U.S. at 11-15; Conn. Gen. Stat. §§ 52-146c, 52-146d, 52-146e, 52-146f, 52-146o (2013).

[535] *E.g.*, §§ 52-146c(c)(3), 52-146f(2).

[536] 20 U.S.C.A. § 1232g (2013); Gonzaga Univ. v. Doe, 536 U.S. 273, 276 (2002).

[537] 20 U.S.C. § 1232g(a)(4)(A).

[538] Owasso Indep. School Dist. v. Falvo, 534 U.S. 426, 431-36 (2002).

[539] 20 U.S.C. § 1232g(d).

[540] 34 C.F.R. § 99.31 (2012 & Supp.).

[541] Uninterrupted Scholars Act (USA), Pub. L. No. 112-278, 126 Stat. 2480 (2013).

[542] *Cf.* Anthony Ciolli, *Grade Non-Disclosure Policies: An Analysis of Restrictions on M.B.A. Student Speech to Employers*, 9 U. Pa. J. Lab. & Emp. L. 709, 723 (2007).

[543] *Gonzaga Univ.*, 536 U.S. at 276.

[544] *Id.* at 289-90; 34 CFR §§ 99.60—99.67 (2012).

[545] Conn. Gen. Stat. § 10-15b (2013); Conn. Gen. Stat. § 10-154a(b) (2013).

[546] 20 U.S.C. § 7908(a)(1) (2006 & Supp. V 2011). A bill has been introduced in Congress regarding release of secondary school students' information to military recruiters with parental consent. *Bill Summary and Status 113th Congress (2013-14) H.R. 392*, Thomas (Library of Congress), http://www.thomas.gov/home/bills_res.html (last visited Mar. 19, 2013). *See generally* Congress-Summary.com, http://www.congress-summary.com/Home.html (last visited Mar. 19, 2013) (providing helpful search tool).

[547] 20 U.S.C. § 7908(d).

[548] 20 U.S.C. § 7908(a)(2).

[549] Mae C. Quinn, *The Fallout from our Blackboard Battlegrounds: A Call for Withdrawal and a New Way Forward*, 15 J. Gender Race & Just. 541, 542, 564 (2012).

[550] Ricky Campbell, *Torrington Scores High in Student Privacy for Military Exams*, Register Citizen, Oct. 26, 2012, http://registercitizen.com/articles/2012/10/26/news/doc508a2806953e1026957450.txt.

[551] Anna M. Schleelein, *The Legal Implications of Unauthorized Promises and Other Military Recruiter Misconduct*, 17 B.U. Pub. Int. L.J. 141, 146 (2007); Phillip Ruben Nava, *Equal Access Struggle: Counter-Military Recruitment on High School Campuses*, 44 J. Marshall L. Rev. 459, 467 n.49 (2011).

[552] 42 U.S.C. §§ 2000aa—2000aa-7 (2006 & Supp. V 2011); David J. Loundy, *E-Law: Legal Issues Affecting Computer Information Systems and Systems Operator Liability*, 3 Alb. L.J. Sci. & Tech. 79, 119 (1993).

[553] Zurcher v. Stanford Daily, 436 U.S. 547 (1978), *superseded by statute as recognized in* Sennett v. United States, 667 F.3d 531, 535 (4th Cir. 2012).

[554] Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 San Diego L. Rev. 843, 858 & n.73 (2002).

[555] 18 U.S.C.A. § 2710 (2013).

[556] Video Privacy Protection Act Amendments Act of 2012, Pub. L. No. 112-258, 6 Stat. 2414 (2013).

[557] Rhodes & Schwab, *supra* note 217, at *10.

[558] Conn. Gen. Stat. § 53-450(a) (2013).

[559] Conn. Gen. Stat. §§ 53-420—53-422 (2013); Conn. Gen. Stat. § 16-331j (2013) (regarding "Video service provider offerings, charges, privacy policy, billing and billing disputes").

[560] § 53-422.

[561] 47 U.S.C. § 551 (2006 & Supp. 2011); Kerr, *supra* note 15, at 855-56.

[562] 15 U.S.C. §§ 6501-6506 (2006 & Supp. 2011); Rhodes & Schwab, *supra* note 217, at *3.

[563] *FTC Resources for Reporters*, Federal Trade Commission, http://www.ftc.gov/opa/reporter/privacy/donottrack.shtml (last visited Mar. 1, 2013). An FTC staff report advises companies to follow this policy. Edward Wyatt, *F.T.C. Suggests Privacy Guidelines for Mobile Apps*, N.Y. Times, Feb. 1, 2013, http://www.nytimes.com/2013/02/02/technology/ftc-suggests-do-not-track-feature-for-mobile-software-and-apps.html?hp&_r=0.

Bills have been introduced in both houses on the subject of commercial tracking through electronic devices. *Bill Summary and Status 113th Congress (2013-14) H.R. 210, S. 418*, Thomas (Library of Congress), http://www.thomas.gov/home/bills_res.html (last visited Mar. 21, 2013). And a bill regarding protection of personal information online has been introduced. *Bill Summary and Status 113th Congress (2013-14) H.R. 1121*, Thomas (Library of Congress), http://www.thomas.gov/home/bills_res.html (last visited Mar. 21, 2013). *See generally* Congress-Summary.com, http://www.congress-summary.com/Home.html (last visited Mar. 19, 2013) (providing helpful search tool).

[564] Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

[565] Schwartz & Solove, *supra* note 456, at 1819-31.

[566] *Id.* at 1818-19, 1836-48.

[567] *Is Your Printer Spying on You?*, Electronic Frontier Found., https://www.eff.org/issues/printers (last visited Feb. 23, 2013).

[568] Schwartz & Solove, *supra* note 456, at 1865-94.

[569] *E.g.*, Nick Wingfield, *Microsoft Attacks Google on Gmail Privacy*, N.Y. Times, Feb. 6, 2013, http://bits.blogs.nytimes.com/2013/02/06/microsoft-attacks-google-on-gmail-privacy/.

[570] *E.g.*, *Facebook and Privacy*, Facebook, https://www.facebook.com/fbprivacy (last visited Mar. 1, 2013).

[571] 15 U.S.C. §§ 7701—7713 (2006 & Supp. V 2011).

[572] 47 U.S.C. § 227 (2006 & Supp. V 2011); Rhodes & Schwab, *supra* note 217, at *7-8.

[573] Conn. Gen. Stat. §§ 53-451(b)(7), 53-452 (2013).

A remedy for the plague of telemarketers is to contact the Connecticut Department of Consumer Protection and ask to be on its do-not-call list. T*he "Do Not Call" Registry and Relevant Laws*, Conn. Dep't of Consumer Prot., http://www.ct.gov/dcp/cwp/view.asp?q=285064 (last visited Mar. 1, 2013).

[574] *E.g.*, 18 U.S.C. § 1028(d)(7) (2006 & Supp. V 2011); Flores-Figueroa v. United States, 556 U.S. 646 (2009).

[575] *Identify Theft*, Fed. Trade Comm'n (Mar. 1, 2013), http://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[576] Conn. Gen. Stat. § 53a-129a (2013).

[577] Conn. Gen. Stat. §§ 53a-129b, 53a-129c, 53a-129d (2013); *see also* Conn. Gen. Stat. § 52-571h (2013).

[578] California v. Greenwood, 486 U.S. 35 (1988); State v. DeFusco, 620 A.2d 746 (Conn. 1993).

[579] *Q&A: Event data recorders*, Ins. Inst. for Highway Safety Highway Loss Data Inst. (Feb. 2013), http://www.iihs.org/research/qanda/edr.aspx.

[580] *Cf.* 49 C.F.R. §§ 563.1—563.12 (2012 & Supp.).

[581] Conn. Gen. Stat. § 14-164aa (2013). There are other exceptions allowing disclosure without the owner's consent, including use in a civil suit. *Id.*

[582] Friedrich, *supra* note 252, at 10-16; Newitz, *supra* note 252, at 17-27; Am. Civil Liberties Union et al., *supra* note 252, at 33-47; Davis, *supra* note 252, at 64-76.

[583] Friedrich, *supra* note 252, at 10-16; Am. Civil Liberties Union et al., *supra* note 252, at 33-47.

[584] Friedrich, *supra* note 252, at 10-16; Am. Civil Liberties Union et al., *supra* note 252, at 33-47.

[585] Friedrich, *supra* note 252, at 10-16; Am. Civil Liberties Union et al., *supra* note 252, at 33-47.

[586] Friedrich, *supra* note 252, at 10-16; Newitz, *supra* note 252, at 17-27; Am. Civil Liberties Union et al., *supra* note 252, at 33-47.

[587] *See* RFID Technology, *supra* note 252, at 1-9; Friedrich, *supra* note 252, at 10-16; Newitz, *supra* note 252, at 17-27; Am. Civil Liberties Union et al., *supra* note 252, at 33-47; Davis, *supra* note 252, at 64-76; Foster & Jaeger, *supra* note 252, at 83-93.

[588] RFID Technology, *supra* note 252, at 1-9.

[589] Davis, *supra* note 252, at 64-76.

[590] The Supreme Court has approved such a law in Indiana. Crawford v. Marion Cnty. Election Bd., 553 U.S. 181 (2008). In Connecticut, you must present some form of identification, but it need not be a photo identification. Conn. Gen. Stat. § 9-261 (2013).

[591] Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Pub. L. No.109–13, 119 Stat. 231 (2005).

[592] *Western Hemisphere Travel Initiative*, U.S. Customs and Border Protection, http://www.getyouhome.gov/html/rfid/RFID.html (last visited Apr. 20, 2013); Allie Bohm, *Yes, the States Really Reject Real ID*, Am. Civ. Liberties Union (Mar. 27, 2012, 3:21 PM), http://www.aclu.org/blog/technology-and-liberty/yes-states-really-reject-real-id.; Paul Frisman, OLR Backgrounder, REAL ID Implementation in Connecticut (Mar. 3, 2011).

[593] In 2012 we successfully opposed Senate Bill No. 288—An Act Requiring a Study of Radio-Frequency Identification for Motor Vehicle Registration.

[594] Newitz, *supra* note 252, at 17-27; Am. Civil Liberties Union et al., *supra* note 252, at 33-47; Davis, *supra* note 252, at 64-76.

[595] Newitz, *supra* note 252, at 17-27; Am. Civil Liberties Union et al., *supra* note 252, at 33-47; Davis, *supra* note 252, at 64-76.

[596] Newitz, *supra* note 252, at 17-27; Am. Civil Liberties Union et al., *supra* note 252, at 33-47; Davis, *supra* note 252, at 64-76.

[597] Am. Civil Liberties Union et al., *supra* note 252, at 33-47.

[598] *Id.*

[599] *Id.*

[600] *Id.*

[601] Florence v. Bd. of Chosen Freeholders of City. of Burlington, 132 S. Ct. 1510, 1513-22 (2012).

[602] *Id.* at 1513-22 (majority opinion); *id.* at 1523 (Roberts, C.J., concurring) (emphasizing warrant and placement in general population); *id.* at 1524 (Alito, J., concurring) (emphasizing placement in general population).

[603] *Id.* at 1520-21.

[604] *Id. at* 1528 (Breyer, J., dissenting).

[605] Conn. Gen. Stat. § 54-33l(a), (b) (2013).

[606] State v. Robinson, 937 A.2d 717, 727-28 (Conn. App. Ct. 2008), *aff'd*, 963 A.2d 59 (Conn. 2009); State v. Jenkins, 842 A.2d 1148, 1155-57 (Conn. App. Ct. 2004).

[607] § 54-33l(g). Even after detention is sanctioned by a court, strip-searches may not be conducted in an unreasonable manner. Bell v. Wolfish, 441 U.S. 520, 559 (1979).

[608] N.G. v. Connecticut, 382 F.3d 225, 226-27 (2d Cir. 2004).

[609] *Id.* at 232.

[610] Safford Unified School Dist. No. 1 v. Redding, 557 U.S. 364, 368 (2009).

[611] *Id.* at 370-77 (citing New Jersey v. T.L.O., 469 U.S. 325 (1985)).

[612] Rebekka Murphy, Note, *Routine Body Scanning in Airports: A Fourth Amendment Analysis Focused on Health Effects*, 39 Hastings Const. L.Q. 915, 920 (2012) (citation omitted) (internal quotation marks omitted); *see also* Erik Luna, *The Bin Laden Exception*, 106 Nw. U. L. Rev. 1489, 1499-1500 (2012).

[613] Murphy, *supra* note 612, at 920-21.

[614] Luna, *supra* note 612, at 1489, 1500.

[615] Scott McCartney, *TSA Pulls Plug on X-Ray Body Scanners Amid Privacy, Health Concerns*, WSJ Blogs (Jan. 22, 2013, 12:02 PM), http://blogs.wsj.com/middleseat/2013/01/22/tsa-pulls-plug-on-x-ray-body-scanners-amid-privacy-health-concerns/.

[616] Elec. Privacy Info. Ctr. v. United States Dep't of Homeland Sec., 653 F.3d 1, 10 (D.C. Cir. 2011) (citing cases).

[617] *Id.* (citing Illinois v. Lidster, 540 U.S. 419 (2004).

[618] *See, e.g.*, United States v. Ramsey, 431 U.S. 606, 616 (1977). Even border searches must be reasonable. United States v. Cotterman, 09-10139, 2013 WL 856292 (9th Cir. Mar. 8, 2013).

[619] Susan Stellin, *Airport Screening Concerns Civil Liberties Groups*, N.Y. Times, Mar. 11, 2013, http://www.nytimes.com/2013/03/12/business/passenger-screening-system-based-on-personal-data-raises-privacy-issues.html?pagewanted=all.

[620] Ferguson v. Charleston, 532 U.S. 67, 79 (2001).

[621] Vernonia School Dist. 47J v. Acton, 515 U.S. 646 (1995); Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656 (1989).

[622] *Ferguson*, 532 U.S. at 78-86.

[623] *Id.*

[624] Skinner v. Railway Labor Execs.' Ass'n, 489 U.S. 602, 608–13 (1989).

[625] *Von Raab*, 489 U.S. at 659.

[626] Chandler v. Miller, 520 U.S. 305 (1997).

[627] *Ferguson*, 532 U.S. at 78-86. Under this special needs analysis, the Court has approved a drunk-driving checkpoint owing to the compelling need for safety, Michigan Dep't of State Police v. Sitz, 496 U.S. 444 (1990), but not a checkpoint where police used drug-sniffing dogs to uncover crime, City of Indianapolis v. Edmond, 531 U.S. 32 (2000).

[628] *Acton*, 515 U.S. at 657.

[629] *Id.* at 658-66.

[630] Bd. of Educ. v. Earls, 536 U.S. 822 (2002).

[631] *Earls*, 536 U.S. at 833; *Ferguson*, 532 U.S. at 78-86.

[632] Conn. Interscholastic Athletic Conference, Handbook 107 § 4.15H (2012-13), *available at* http://www.casciac.org/pdfs/ciachandbook_1213.pdf. This handbook came to our attention from a high-school student's article, reprinted at DJ Sixsmith, *High School Drug Testing, To Test or Not to Test*, Westport Patch (Apr. 25, 2011), http://westport.patch.com/articles/high-school-drug-testing-to-test-or-not-to-test.

[633] Conn. Gen. Stat. § 54-33n (2013); Burbank v. Canton Bd. of Educ., No. CV094043192S, 2009 WL 3366272 (Conn. Super. Ct. Sept. 14, 2009), *appeal dismissed*, 11 A.3d 658 (Conn. 2011).

[634] Alderman & Kennedy, *supra* note 4, at 24-25.

[635] Hayes v. Florida, 470 U.S. 811 (1985).

[636] *Cf.* N.Y. Civil Liberties Union, *supra* note 8, at 12; Mai, *supra* note 183; *see also* Dillow, *supra* note 183.

[637] 5 U.S.C. § 9101 (2006 & Supp. V 2011); 7 U.S.C. § 12a (2006 & Supp. V 2011); 8 U.S.C. §§ 1101, 1105 (2006 & Supp. V 2011); 12 U.S.C. § 5104 (2006 & Supp. V 2011); 18 U.S.C. § 843 (2006 & Supp. V 2011); 18 U.S.C. § 923 (2006 & Supp. V 2011); 42 U.S.C. § 1320a-7l (2006 & Supp. V 2011); 42 U.S.C. § 2169 (2006 & Supp. V 2011); 42 U.S.C. § 5119a (2006 & Supp. V 2011); 42 U.S.C. § 13701 (2006 & Supp. V 2011); 42 U.S.C. § 16914 (2006 & Supp. V 2011); 49 U.S.C. § 5103a (2006 & Supp. V 2011); 49 U.S.C. § 40130 (2006 & Supp. V 2011); 29 U.S.C. § 1812 (2006 & Supp. V 2011); 18 U.S.C. § 4082 (2006 & Supp. V 2011); 18 U.S.C. § 5038 (2006 & Supp. V 2011).

[638] Conn. Gen. Stat. §§ 29-11, 29-12, 29-15 (2013); Conn. Gen. Stat. § 46b-133 (2013).

[639] § 29-12.

[640] *Id.*; Conn. Gen. Stat. § 54-250 (2013).

[641] Conn. Gen. Stat. §§ 29-29, 29-36g (2013).

[642] Conn. Gen. Stat. § 36a-488 (2013); Conn. Gen. Stat. §36a-437a (2013); Conn. Gen. Stat. § 36a-70 (2013); Conn. Gen. Stat. § 31-130 (2013); § 29-12; Conn. Gen. Stat. § 10-221d (2013); Conn. Gen. Stat. § 13b-97 (2013); § 29-11; Conn. Gen.

Stat. §§ 29-155, 29-161k (2013); Conn. Gen. Stat. §§ 14-44, 14-69 (2013); Conn. Gen. Stat. § 17a-115a (2013); Conn. Gen. Stat. § 14-9a (2013); Conn. Gen. Stat. § 29-145 (2013); Conn. Gen. Stat. § 29-349 (2013).

[643] Michael J. Crook, *Sacrificing Liberty for Security: North Carolina's Unconstitutional Search and Seizure of Arrestee DNA*, 34 Campbell L. Rev. 473, 508 (2012).

[644] Haskell v. Harris, 669 F.3d 1049, 1053 (9th Cir. 2012), *reh'g en banc granted*, 686 F.3d 1121 (9th Cir. Jul 25, 2012); United States v. Amerson, 483 F.3d 73, 77 (2d Cir. 2007).

[645] Maryland v. King, 133 S. Ct. 1, 2-3 (2012) (Roberts, Cir. J.) (citing cases); Maryland v. King, 133 S. Ct. 594 (2012) (granting cert.).

[646] 18 U.S.C. § 3142(b), (c)(1)(A) (2006 & Supp. V 2011); 42 U.S.C. § 14135a (2006 & Supp. V 2011).

[647] Conn. Gen. Stat. § 54-102g (2013).

[648] *Id.*

[649] *Id.*

[650] Conn. Gen. Stat. §§ 54-102g—54-102m (2013).

[651] 42 U.S.C. §§ 2000ff—2000ff-11 (2006 & Supp. V 2011).

[652] Conn. Gen. Stat. § 46a-60(11) (2013).

[653] *Griswold*, 381 U.S. 479.

[654] Conn. Gen. Stat. §§ 53-31, 53-31a, 53-31b (repealed).

[655] *Roe*, 410 U.S. 113.

[656] *Id.* at 163-64.

[657] *Planned Parenthood of Se. Penn.*, 505 U.S. at 874 (modifying *Roe*, 410 U.S. 113).

[658] Conn. Gen. Stat. § 19a-602 (2013).

[659] *Roe*, 410 U.S. at 163.

[660] Conn. Gen. Stat. § 19a-116 (2013); Conn. Gen. Stat. §§ 19a-600, 19a-601 (2013).

[661] Conn. Gen. Stat. § 10-16c (2013).

American Civil Liberties Union of Connecticut

330 Main Street Hartford, CT 06106

acluct.org