Digital Privacy: Leibniz 2.0

Wade L. Robison
Rochester Institute of Technology

Corresponding Author: Wade L. Robison, wade.robison@gmail.com

Abstract

In 1963, Chief Justice Earl Warren called the ‘fantastic advances in the field of electronic communication’ a danger to the privacy of the individual. If we use the privacy torts as developed in American law — intrusion, disclosure, false light, appropriation — we can see how dangerous those advances have been regarding our privacy. We will see how readily so many can do so much more to invade the privacy of so many more. We will also see a thread running through the privacy torts that was not readily visible before: invasions of privacy treat us as objects to be observed, revealed, manipulated, and used.

Keywords: privacy, intrusion, disclosure, false light, appropriation, objects

Introduction

In a 1963 United States Supreme Court tax fraud case involving a wire recording, Chief Justice Earl Warren wrote, ‘The fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual’ — greater than an IRS agent rifling a defendant’s desk, for instance (Warren, 1963). The Chief Justice would no doubt be astonished at how ‘the field of electronic communication’ has burgeoned in the last half century and would be even more concerned than he was in 1963 about the dangers to individual privacy.

It is easy to go astray in exploring those dangers by trying to begin with a definition of privacy. The definitions most cited tie the concept to a particular form of invasion. So ‘the right to be left alone’ fits nicely with the notion that intrusion is the fundamental form of invasions of privacy, but that leaves out other forms of invasion of privacy, e.g., disclosure. So beginning with any traditional definition of privacy invites a question-begging narrowing of our understanding of privacy.

In addition, I shall argue, we will gain a new understanding of what grounds our concerns about privacy by examining the effects of the digital revolution. Definitions that appeal to what used to be the paradigmatic examples of invasions of privacy are no longer general enough, or accurate enough, to capture what it means to have one’s privacy invaded electronically. As I shall argue, we can now come to an understanding that grounds all the ways in which privacy can be invaded — something much harder to see before the digital revolution and part of the reason for the disagreement about what privacy means, as each definition focused on one or another of the various ways in which our privacy can be invaded.

So I will assume that we all can give unproblematic examples of how our privacy can be invaded, showing
that we can use the concept without difficulty, and I will leave any discussion of what undergirds the concept — why invasions of privacy are treated as harms — until after we discuss its fate in the digital age.

I will begin with the privacy torts in the United States — not to elevate them over the legal understandings in other countries, but to take advantage of the more than century-old development of those torts in case law. There is a great deal to be said in favor of an understanding honed in case after case where new circumstances call for modifications of a previous conception.

I will then make a detour into Leibniz’s metaphysics to pull out several features that will help us understand the ways in which ‘the field of electronic communication’ has radically altered our privacy. I will use it to introduce Leibniz 2.0 and explain how I think our privacy has been so radically altered.

### Privacy Torts

In 1890 Warren and Brandeis published an article on privacy in the *Harvard Law Review*. Warren was incensed that newspaper reporters had crashed his daughter’s wedding, making it a public event with their articles and photographs, and he and Brandeis argued there was a right to privacy that ought to be recognized and protected by the law (Warren, 1890). That right to privacy turned out to be complex, giving rise to four different torts and a constitutional right.

What is of interest in this digital age is that the four privacy torts correspond to four different kinds of harm that have become more extensive because of the rise of digital devices and our new forms of communication and commercial transactions.

The four privacy torts are intrusion, disclosure, false light and appropriation. They seem to cover the full scope of how privacy can be invaded — although I shall not provide any argument to justify that claim. I will also, as I said, rely on our common understanding of what privacy means as I briefly explain the four privacy torts (Prosser, 1960).

When the tort of intrusion was being recognized in case law, the paradigmatic example was of someone barging in on some person or set of persons, uninvited — coming into your bedroom while you were engaged in making love, opening the broken toilet stall door and standing there, leaning against it, while you finished up, peeking into your window as you undressed. In this paradigmatic kind of case, intrusion required the physical presence of another person in a space appropriately designated as private by those within it. This is the paradigm that explains the visceral response to intrusion — anger, humiliation, shame, the responses that powered resort to the courts for protection and damages.

Marginal to this paradigmatic example, historically, were those situations where someone intruded without being physically visible — by setting up mirrors in one’s own yard to spy on a neighbor, for instance, through a telescope in one’s living room. The harm that comes from intrusion does not depend upon our knowing someone has intruded. A peeping Tom could peep undetected. But on the old paradigm intrusion does require that there be someone there, physically present, who could be discovered and so could be blocked by pulling the blinds, for instance.

Disclosure does not require our discovery that what we thought private has been disclosed. I may tell a friend a secret, asking that they promise to keep it a secret, and yet my friend passes it on — without my necessarily realizing others now know. What is required is that something we thought was accessible only to ourselves and those we let into our world be made public in some way to others not part of our world — to others to whom we are neither intimate nor perhaps even acquainted. The harm comes from others being informed of
something that we had meant to keep to ourselves or to a small group. We can imagine the harm that would be done if the secret I tell my friend is that I am breaking up with my partner and my partner discovers that through a third party and not from me.

False light may seem like an odd privacy tort. It occurs when someone says or implies something false about your private life. ‘Don’t let him get near your young girls without your being present!’ ‘He cheats on his partner whenever he can.’ Someone aiming to harm another would pick an attribution that fits the person’s] character — ‘He does show an odd interest in young girls.’ The harm could occur with the person remaining unaware of the attribution since no one is likely to say anything about it. Why say anything? The person would deny it even if it were true and be warned as a consequence of your saying something about it. False light would be even more perverse if the person could falsity the false light only by revealing something private the person would never have revealed otherwise (Robison, 1997).

Appropriation may seem like another odd privacy tort. In these cases, someone or some company takes another’s identity. The law started with such mundane cases as a photographer selling a photograph of a young socialite to a flour company to put on their flour sacks under the motto, ‘The Flower of Flours’ (Robertson, 1902). We are most familiar with cases of identity theft or impersonation — someone masquerading as someone else. The gain may be monetary, but need not be. Someone posed as Vidal, the fashion photographer, with the aim of bedding the young women he convinced to be photographed with the promise that he would send the photos to fashion magazines (The phony photographer, 1997).

Those are the four privacy torts, and, I shall argue, they have become more extensive in the digital age — putting us all at greater risk of having what we may have thought private, or wanted to keep private, become available to others who would not normally be privy to such material.

**Excursus into Leibniz**

It may seem odd to turn to a 17th-century philosopher with a decidedly quirky metaphysical system to get clarity on how the digital age has affected privacy, but Leibniz would be right at home in this digital age, and, with some tweaking, his understanding of the nature of an individual gives us an insight into how our sense of privacy has changed.

Leibniz says that ‘the nature of an individual substance or of a complete being is to have a notion so complete that it is sufficient to comprise and to allow the deduction from it of all the predicates of the subject to which this notion is attributed’ (Leibniz, 1953). The idea Leibniz has here is relatively straightforward, whatever one may think of its truth or falsity. My identity as a person — ‘an individual substance or...a complete being’ — just is the complete set of predicates that are true of me. That I am sitting here by a fire as I write this, that I can see the cat out of the corner of my eye and one of the dogs laying nearby, that I made soup for my dinner this evening followed by a piece of homemade mixed-berry pie for dessert — all these predicates are true of me. Although that particular string is general enough that it could be true of another being, or true of me some other evening, we can readily add more specificity to make it uniquely mine.

We can add the necessary specificity by expanding the predicates. It is not just any homemade mixed-berry pie I had, but the one here, at this house, on this evening, with homegrown raspberries, blueberries, and blackberries — and so on until we get enough expansive predicates to be sure we have individuated the piece of pie I had. It is this fire I am sitting next to, the one with the locust logs from our woods I cut and split and stacked behind the house and then hauled in from the wood pile. We could just add more and more details to the predicates, that is, until we have isolated the individual substance in question from every other substance in the world.
We could also add the necessary specificity by adding more predicates without worrying overly much about how specific they are. Get all the predicates that are true of me, and you will have zeroed in on me; the longer the string, the less likely you will latch onto any doppelgänger. Indeed, Leibniz argues, no two substances, or strings of predicates, can have identical predicates. I cannot have an identical doppelgänger.

Leibniz claims that all the predicates of an individual are deducible from its complete notion, that they are necessarily connected. But he is mistaken about that. Each predicate is only contingently related to any other. Leibniz also claims that God is aware of all predicates. He denies the reality of relations, but if we ignore that mistake, we can say that each predicate in each substance or complete being always has, as it were, a relation to God. It is not just true of me that I had a piece of mixed-berry pie for dessert, but that I had a piece of pie and while having it, God was watching. An additional feature of Leibniz’s quirky metaphysical system is that all predicates are of a kind. Ontologically, there is no difference between one predicate and another. Nothing stands out as true of me, for instance, that makes me who I am. I and everything else have been, as it were, ontologically flat lined: every being is just one predicate after another.

**Leibniz 2.0**

Let us replace Leibniz’s predicates with 1’s and 0’s. This is Leibniz 2.0, and here is what Leibniz would say of our metaphysical digital world:

1. Each individual being is a string of 1’s and 0’s.
2. Each string for each individual being is unique: identical strings are indiscernible.
3. Each bit of string, however short, even each 0 and each 1, can be in a relation to some other string or strings: either God or the NSA or some other entity may be watching it.

Because the relations between the digits are contingent, we cannot deduce anything from any digit or any string of digits. Leibniz thinks such deductions are possible in his world, for God, but in our world, with Leibniz 2.0, no one digit contains, to use his word, any other digit. Each is contingent, and each string is contingent, whatever its length.

In addition, a string can be exceedingly complex, covering not just something we do or feel or think, for instance, but also containing relations to others. The relations are contingent, just as are the relations between digits: a peeping Tom may fail in his endeavors, but when successful, the digits relating what is going on when he succeeds are part of the complex string that marks out what the peepees, if I may call them that, are doing.

So when intrusion occurs, we have a longer string than when it does not. I suggested in regard to Leibniz 1.0 that we can zero in on a particular individual by expanding each predicate true of that individual so that it includes e.g., spatial/ temporal coordinates. We can also zero in on someone in Leibniz 1.0 by adding more predicates: ‘Wade is that individual who…’, adding what is needed about me to zero in on me, excluding every other individual being. That distinction is tenuous in Leibniz 1.0 and completely lost in 2.0. Expanding the digits just is to add more digits. I turn out to be quite a long string — not infinite, obviously, but longer than anyone could possibly memorize and unique enough, if only because of the specificity of its length, to pick me out of a crowd.

With the digital age, no one need remember any part of that string. Parts of it are stored away in the cloud or my Mac or my iPhone or my backup — or all of them. Enough are readily accessible by me and by anyone else who can hack into my digital life to focus in on me alone.

So intrusion takes on a different look than it had before the digital age. The paradigmatic example is not of
someone physically present who has come into a space considered private. No one need be physically present at all. And although in the old paradigmatic case, that physical presence was discoverable, if not discovered, and preventable, if not prevented, we face three problems in the digital age in protecting ourselves against intrusion that we did not face before.

First, we have an epistemic shortfall. We do have selfies, and we have individuals posting all manners of things we would have thought they would have preferred to be private — of videos posted online by the perpetrators of rapes, for instance (Blidner, 2015). So we have an epistemic windfall as well, getting more information about more things than perhaps we ever wanted to know. But it is the shortfall that is more significant regarding privacy. The digital age has ushered in ways of intruding upon our privacy that do not require the physical presence of anything we can readily notice. There is Cayla, the talking — and listening — doll (Naylor, 2016; Internet-Connected Toys Are Spying on Kids, Threatening Their Privacy and Security). There is software for taking over the camera in our computers (Cheng, 2010; Kravets, 2012). There is software for hacking into keyboards and mice (Greenberg, 2016). The list is long and gets longer and longer.

In none of these situations do we have any indication that anyone has intruded on our privacy. Unlike the paradigmatic examples from the pre-digital age, we are clueless. We have no one standing at our window, peering in. We have instead our computers un-intrusively, if I may put it that way, taking videos of what we are doing and relaying them to someone far away from us.

Second, most of us also have an epistemic shortfall about the technology being used to intrude on our privacy. I would suspect that a random survey of digital users — cell phones, tablets, computers, wifi-enabled electronic equipment such as thermostats — would find few familiar with many, even any, of the ways information about them can be gathered and stored. Accessing keyboards? Who knew? In retrospect, we can realize that our computers, for instance, are unique, each with its own history, use of fonts, webpages regularly browsed, and so on. Each has a fingerprint, as the terminology now puts it, and so those interested in accessing your computer can know exactly which computer to single out (Avirgan, 2016). But such information comes as a discovery for most of us, not a prediction we could have made even after long use of a computer keyboard.

Third, with those two epistemic shortfalls, we can, at best, only protect ourselves in a general way — turning off our computers when we are not using them so others cannot access them and make use of them when we are not, turning off GPS on those apps we do not need it for, making sure we have two-step identification, having complicated passwords which we change often. That people in general do not take these precautions is a given. It is also a given that even if we do, we are still vulnerable in ways we might not suspect — and will no doubt become vulnerable in new unexpected ways as the number and variety of our digital gadgets increase and more software, with its inevitable hackable holes, permeates our lives.

So here is where we are with intrusion. We have a new paradigm in which we go about our lives completely unaware that anyone is intruding, but always at risk of having some entity intrude. In Leibniz 1.0, God is always there as our predicates unfold. In Leibniz 2.0, we cannot know if the NSA or some person or other agency or corporation is there. What we can know is that we are always at risk of intrusions that we cannot be aware of.

Indeed, almost anyone could be intruding on our privacy. It is now far easier than it used to be. No one needs to find a room to barge into. Anyone can hire a firm that will infest a person’s cellphone, recording everything said on it or done with it, including its location. Anyone can get an app for tracking cellphones, for instance — less intrusive, but still intrusive — and it does not cost a dime.
With the old paradigm, our reactions to intrusions — anger, humiliation, shame — powered the legal cases. The law was built case-by-case by individuals suing to protect what they claimed was private. With this new paradigm, these reactions are missing simply because of the epistemic shortfall that leaves us unaware of any intrusion. As Leibniz 2.0 makes clear, we are flat lined, just 0’s and 1’s, and nothing in that flat line of digits stands out in the way in which someone bursting into our bedroom stands out.

So intrusions in this digital age are more likely, but also significantly more difficult to detect. One unfortunate mode of detection comes from the disclosure of what has been uncovered through intrusion, and it is now far easier to disclose what was supposed to be private and disclose it to more than just a friend. The old paradigm was that you tell a friend a secret, which is then disclosed to someone else, the circle of those in the know widening, perhaps, but usually a relatively small number. Now it goes on Facebook, or the video goes on YouTube, or the information you wanted private goes up on a webpage — open to far more individuals than it would have been, millions perhaps instead of a small circle.

Again, Leibniz 2.0 makes it all so easy. Videos, porno, email messages, diaries on laptops — it is all just 1’s and 0’s, easily sent anywhere in the world or uploaded to a website for all to see. We have the confluence of three basic presumptive principles governing the digital age:

• Everything can be digitized.
• Anything digital can go public.
• It is relatively easy for anyone to make it public, even young children.

I call these presumptive to mark their status. I am not arguing that they are empirically true, but that we should presume their truth in this digital age.

Such presumptions are relevant for all the privacy torts. False light? Anyone can select some set of digits that are false of your private life and so insert them into your digital chain that they look to be true — by putting them on Facebook, or sending an email to an acquaintance, or, if you are famous, sending it onto some news media for them to publish. You have then been put into a false light, and if anyone cares, disclosure will soon follow, with all the attendant complications to your life.

The same is true of appropriation. Almost anyone can latch onto enough of your digital string to appropriate enough of your identity to masquerade as you — buying what they want in ‘your’ name with ‘your’ credit card or bank loan, for instance. Identity theft is on the increase, and we can expect far more of it.

So what has changed regarding privacy in the digital age? The harms have not changed. We would still sue on the same grounds as we did before the ‘fantastic advances in the field of electronic communication.’ Intrusion occurs when someone gains access to a space or place when they have no right of access. Disclosure occurs when someone makes public information, photos, videos, and so on when they have no right to make that public. False light occurs when someone inserts something false about our private life into our digital string — and so potentially misleads others. Appropriation occurs when others take on our digital string, or enough of it, to present themselves as us.

What has changed? What has changed is that invasions of privacy are more:

• penetrating because much of what we would have thought inaccessible before is now readily accessible or nearly so, with information about our purchases, our locations, our personal emails and so on much easier for others to obtain;
pervasive since anything about us may be disclosed to a far larger public, and more can spread false light and appropriate our identities; and
extensive because anyone with a real interest in invading a person’s privacy now has the means to do so.

A larger amount of information can now be made available to a larger number of people by a larger number of people.

**A new world: ‘If this is the best of all possible worlds, what are the others like?’**

It is only going to get worse. It is one mark of our new world that we seem to be moving towards a cashless society. Sweden is clearly the leader in this regard (Heller, 2016), but the increasingly heavy use of debit cards as well as credit cards means that much of our digital strings will become housed in clouds, accessible to any with the wherewithal to penetrate them and retrieve what they need. Despite the convenience to individuals of not having to bother with cash, it is not obvious that an arrangement that leaves such a detailed trail of one’s commercial life is the best of all possible worlds.

So what are the harms? They are, first, a multitude of the old harms: more intrusions by more people and by corporations and government agencies; more disclosure of more intimate details of our lives to more people by more people; more false light that, once broadcast about, is nearly impossible to correct; and more appropriation, especially in the form of identity theft. These are not trivial harms in and of themselves, and when they come in a steady flow — one identity theft after another, say — they can overwhelm our lives, forcing us to spend countless hours, weeks, months, even years trying to get our credit back, for instance.

But there is a deeper and more disturbing harm that Leibniz 2.0 helps reveal. I began by remarking on how difficult it is to find a neutral definition of privacy, one that does not take its meaning from a particular privacy tort. Part of the difficulty is that the harms that result from invasions of privacy vary from tort to tort. It is one thing to have someone break into a bedroom to witness a couple making love and quite another to post videos of them. They are both invasions of privacy, but the harms seem far different. On the one hand, the intrusion interrupts the couple’s love-making, puts both in an embarrassing position, if I may put it that way, and has implications for their future activities (like checking that the door is locked). If the intruder is known to one or both, their relationships have now changed, presumably not for the better. On the other hand, the intruder’s disclosing what was witnessed makes the couple a public spectacle, producing embarrassment and shame presumably, but also altering the couple’s public personae, how all those who have seen what was disclosed now relate to them and thus how they themselves alter how they relate to all those they meet, not knowing if they have seen the disclosure or not.

There may seem little in common between these two sets of privacy harms, and that is one explanation for the difficulty in agreeing on a neutral definition. But Leibniz 2.0 lets us see one common harm that holds for all the privacy torts, false light and appropriation included. Recall that in Leibniz 1.0, God is always there, watching, as it were, and that we have no control over who we are or what we do: God chooses which beings are to come into existence, and all a being’s predicates are to be deduced from the concept of that being. We have an illusory semblance of free will for Leibniz, I would argue, but the reality for him is that each predicate is deducible from the complete notion of any being. So no beings have any power to control anything about themselves. In Leibniz’s metaphysics, we are objects, playing out our lives because God has chosen that we exist and in making that choice, has thereby chosen all the predicates that are true of us and none that are not.
Leibniz claims this the best of all possible worlds. Otherwise, he asks, why would God have chosen to bring it into existence? But in his world, we are being treated by God as means to an end. We have no control over our lives because the world would not be the best were what God has chosen to change in any way. But this is an unethical world – at least in Kant’s view.

It is central to Kant’s ethics that we are not to use others. Even if slavery were somehow to produce the greatest good for the greatest number, or the best of all possible worlds, it would be morally impermissible because slaves would be instruments for the benefit of others. We are not to treat others as objects for our benefit or the benefit of the whole. Persons deserve respect as beings capable of making their own choices.

Treating others with respect and not as objects is an heuristic ideal, obviously. Too many do too much that is wrong to too many for anyone to claim that we live in Kant’s ideal world. But the crucial change in the digital age is that we can now, far more easily, treat each other as objects to be observed, revealed, manipulated, and used. With some training and often very little expense, we can gain access to almost anyone’s digital string, intruding without their knowledge on what they are doing and thinking (so long as that is expressed), disclosing with almost God-like ease what we wish of what we observe, and, again with God-like ease, inserting what we wish into anyone’s string or taking what we wish from it as our own. If we are willing to pay, we can hire companies that will install software on your phone, turning it into a recording device, bypassing encryption, with ‘all the data [being] sent back to the agency’s server in real time’ (Perlroth 2016).

What is at issue is our autonomy, our having control over our lives. When someone intrudes on our privacy, the core harm is our loss of control: we did not invite the person in. The effects are humiliation and shame and anger, but what matters is that when intrusion occurs, we have lost control over the relations we have with others. The same is true for disclosure. I tell my intimates things I do not tell strangers, but if others are in on what I say or do, then I no longer have control over the relations I have with others — with whom I let into my circle and whom I exclude. The same loss of control is even more obvious with the privacy torts of false light and appropriation. Someone is manipulating who I am, as it were, with false light, changing how I seem to others. We all present ourselves in certain ways, and for many, if not most, of us, we distinguish between our public and our private persona. What we present ourselves as is obviously not necessarily who we are in private. But false light represents us in a way we cannot control. Our public persona has suddenly become whatever is falsely said of us and believed. Appropriation? We have there lost control over our identity: our string, or enough of it, has been taken over by someone else.

The digital age has made us mini-gods, capable of treating far more, far more easily, as objects. Kant’s vision of an ideal world where we treat each other with respect is that much more difficult to achieve when treating others as objects is so much easier.

References
Avirgan, Jody (2016, September 2). Internet Tracking Has Moved Beyond Cookies. FiveThirtyEight.


Cheng, Jacqui (2010, August 2). Parents: school used webcam to spy on our kid at home. ArsTechnica.


Naylor, Brian (2016, December 20). This Doll May Be Recording What Children Say, Privacy Groups Charge. NPR.


The phony photographer (1997, September 19). Newsweek, 43.
