THE CHRONICLE
of Higher Education
The Chronicle Review

May 15, 2011

Why Privacy Matters Even if You Have 'Nothing to Hide'

By Daniel J. Solove

When the government gathers or analyzes personal information, many people say they're not worried. "I've got nothing to hide," they declare. "Only if you're doing something wrong should you worry, and then you don't deserve to keep it private."

The nothing-to-hide argument pervades discussions about privacy. The data-security expert Bruce Schneier calls it the "most common retort against privacy advocates." The legal scholar Geoffrey Stone refers to it as an "all-too-common refrain." In its most compelling form, it is an argument that the privacy interest is generally minimal, thus making the contest with security concerns a foreordained victory for security.

The nothing-to-hide argument is everywhere. In Britain, for example, the government has installed millions of public-surveillance cameras in cities and towns, which are watched by officials via closed-circuit television. In a campaign slogan for the program, the government declares: "If you've got nothing to hide, you've got nothing to fear." Variations of nothing-to-hide arguments frequently appear in blogs, letters to the editor, television news interviews, and other forums. One blogger in the United States, in reference to profiling people for national-security purposes, declares: "I don't mind people wanting to find out things about me, I've got nothing to hide! Which is why I support [the government's] efforts to find terrorists by monitoring our phone calls!"

The argument is not of recent vintage. One of the characters in Henry James's 1888 novel, *The Reverberator,* muses: "If these people had done bad things they ought to be ashamed of themselves and he couldn't pity them, and if they hadn't done them there was no need of making such a rumpus about other people knowing."

I encountered the nothing-to-hide argument so frequently in news interviews, discussions, and the like that I decided to probe the

issue. I asked the readers of my blog, Concurring Opinions, whether there are good responses to the nothing-to-hide argument. I received a torrent of comments:

- My response is "So do you have curtains?" or "Can I see your credit-card bills for the last year?"
- So my response to the "If you have nothing to hide ... " argument is simply, "I don't need to justify my position. You need to justify yours. Come back with a warrant."
- I don't have anything to hide. But I don't have anything I feel like showing you, either.
- If you have nothing to hide, then you don't have a life. Show me yours and I'll show you mine.
- It's not about having anything to hide, it's about things not being anyone else's business.
- Bottom line, Joe Stalin would [have] loved it. Why should anyone have to say more?

On the surface, it seems easy to dismiss the nothing-to-hide argument. Everybody probably has something to hide from somebody. As Aleksandr Solzhenitsyn declared, "Everyone is guilty of something or has something to conceal. All one has to do is look hard enough to find what it is." Likewise, in Friedrich Dürrenmatt's novella "Traps," which involves a seemingly innocent man put on trial by a group of retired lawyers in a mock-trial game, the man inquires what his crime shall be. "An altogether minor matter," replies the prosecutor. "A crime can always be found."

One can usually think of something that even the most open person would want to hide. As a commenter to my blog post noted, "If you have nothing to hide, then that quite literally means you are willing to let me photograph you naked? And I get full rights to that photograph—so I can show it to your neighbors?" The Canadian privacy expert David Flaherty expresses a similar idea when he argues: "There is no sentient human being in the Western world who has little or no regard for his or her personal privacy; those who would attempt such claims cannot withstand even a few minutes' questioning about intimate aspects of their lives without capitulating to the intrusiveness of certain subject matters."

But such responses attack the nothing-to-hide argument only in its most extreme form, which isn't particularly strong. In a less extreme form, the nothing-to-hide argument refers not to all personal information but only to the type of data the government is likely to collect. Retorts to the nothing-to-hide argument about exposing people's naked bodies or their deepest secrets are relevant only if the government is likely to gather this kind of information. In many instances, hardly anyone will see the information, and it won't be disclosed to the public. Thus, some might argue, the privacy interest is minimal, and the security interest in preventing terrorism is much more important. In this less extreme form, the nothing-to-hide argument is a formidable one. However, it stems from certain

faulty assumptions about privacy and its value.

To evaluate the nothing-to-hide argument, we should begin by looking at how its adherents understand privacy. Nearly every law or policy involving privacy depends upon a particular understanding of what privacy is. The way problems are conceived has a tremendous impact on the legal and policy solutions used to solve them. As the philosopher John Dewey observed, "A problem well put is half-solved."

Most attempts to understand privacy do so by attempting to locate its essence—its core characteristics or the common denominator that links together the various things we classify under the rubric of "privacy." Privacy, however, is too complex a concept to be reduced to a singular essence. It is a plurality of different things that do not share any one element but nevertheless bear a resemblance to one another. For example, privacy can be invaded by the disclosure of your deepest secrets. It might also be invaded if you're watched by a peeping Tom, even if no secrets are ever revealed. With the disclosure of secrets, the harm is that your concealed information is spread to others. With the peeping Tom, the harm is that you're being watched. You'd probably find that creepy regardless of whether the peeper finds out anything sensitive or discloses any information to others. There are many other forms of invasion of privacy, such as blackmail and the improper use of your personal data. Your privacy can also be invaded if the government compiles an extensive dossier about you.

Privacy, in other words, involves so many things that it is impossible to reduce them all to one simple idea. And we need not do so.

In many cases, privacy issues never get balanced against conflicting interests, because courts, legislators, and others fail to recognize that privacy is implicated. People don't acknowledge certain problems, because those problems don't fit into a particular one-size-fits-all conception of privacy. Regardless of whether we call something a "privacy" problem, it still remains a problem, and problems shouldn't be ignored. We should pay attention to all of the different problems that spark our desire to protect privacy.

To describe the problems created by the collection and use of personal data, many commentators use a metaphor based on George Orwell's *Nineteen Eighty-Four*. Orwell depicted a harrowing totalitarian society ruled by a government called Big Brother that watches its citizens obsessively and demands strict discipline. The

Orwell metaphor, which focuses on the harms of surveillance (such as inhibition and social control), might be apt to describe government monitoring of citizens. But much of the data gathered in computer databases, such as one's race, birth date, gender, address, or marital status, isn't particularly sensitive. Many people don't care about concealing the hotels they stay at, the cars they own, or the kind of beverages they drink. Frequently, though not always, people wouldn't be inhibited or embarrassed if others knew this information.

Another metaphor better captures the problems: Franz Kafka's *The Trial*. Kafka's novel centers around a man who is arrested but not informed why. He desperately tries to find out what triggered his arrest and what's in store for him. He finds out that a mysterious court system has a dossier on him and is investigating him, but he's unable to learn much more. *The Trial* depicts a bureaucracy with inscrutable purposes that uses people's information to make important decisions about them, yet denies the people the ability to participate in how their information is used.

The problems portrayed by the Kafkaesque metaphor are of a different sort than the problems caused by surveillance. They often do not result in inhibition. Instead they are problems of information processing—the storage, use, or analysis of data—rather than of information collection. They affect the power relationships between people and the institutions of the modern state. They not only frustrate the individual by creating a sense of helplessness and powerlessness, but also affect social structure by altering the kind of relationships people have with the institutions that make important decisions about their lives.

Legal and policy solutions focus too much on the problems under the Orwellian metaphor—those of surveillance—and aren't adequately addressing the Kafkaesque problems—those of information processing. The difficulty is that commentators are trying to conceive of the problems caused by databases in terms of surveillance when, in fact, those problems are different.

Commentators often attempt to refute the nothing-to-hide argument by pointing to things people want to hide. But the problem with the nothing-to-hide argument is the underlying assumption that privacy is about hiding bad things. By accepting this assumption, we concede far too much ground and invite an unproductive discussion about information that people would very likely want to hide. As the computer-security specialist Schneier

aptly notes, the nothing-to-hide argument stems from a faulty "premise that privacy is about hiding a wrong." Surveillance, for example, can inhibit such lawful activities as free speech, free association, and other First Amendment rights essential for democracy.

The deeper problem with the nothing-to-hide argument is that it myopically views privacy as a form of secrecy. In contrast, understanding privacy as a plurality of related issues demonstrates that the disclosure of bad things is just one among many difficulties caused by government security measures. To return to my discussion of literary metaphors, the problems are not just Orwellian but Kafkaesque. Government information-gathering programs are problematic even if no information that people want to hide is uncovered. In *The Trial,* the problem is not inhibited behavior but rather a suffocating powerlessness and vulnerability created by the court system's use of personal data and its denial to the protagonist of any knowledge of or participation in the process. The harms are bureaucratic ones—indifference, error, abuse, frustration, and lack of transparency and accountability.

One such harm, for example, which I call aggregation, emerges from the fusion of small bits of seemingly innocuous data. When combined, the information becomes much more telling. By joining pieces of information we might not take pains to guard, the government can glean information about us that we might indeed wish to conceal. For example, suppose you bought a book about cancer. This purchase isn't very revealing on its own, for it indicates just an interest in the disease. Suppose you bought a wig. The purchase of a wig, by itself, could be for a number of reasons. But combine those two pieces of information, and now the inference can be made that you have cancer and are undergoing chemotherapy. That might be a fact you wouldn't mind sharing, but you'd certainly want to have the choice.

Another potential problem with the government's harvest of personal data is one I call exclusion. Exclusion occurs when people are prevented from having knowledge about how information about them is being used, and when they are barred from accessing and correcting errors in that data. Many government national-security measures involve maintaining a huge database of information that individuals cannot access. Indeed, because they involve national security, the very existence of these programs is often kept secret. This kind of information processing, which blocks subjects'

knowledge and involvement, is a kind of due-process problem. It is a structural problem, involving the way people are treated by government institutions and creating a power imbalance between people and the government. To what extent should government officials have such a significant power over citizens? This issue isn't about what information people want to hide but about the power and the structure of government.

A related problem involves secondary use. Secondary use is the exploitation of data obtained for one purpose for an unrelated purpose without the subject's consent. How long will personal data be stored? How will the information be used? What could it be used for in the future? The potential uses of any piece of personal information are vast. Without limits on or accountability for how that information is used, it is hard for people to assess the dangers of the data's being in the government's control.

Yet another problem with government gathering and use of personal data is distortion. Although personal information can reveal quite a lot about people's personalities and activities, it often fails to reflect the whole person. It can paint a distorted picture, especially since records are reductive—they often capture information in a standardized format with many details omitted.

For example, suppose government officials learn that a person has bought a number of books on how to manufacture methamphetamine. That information makes them suspect that he's building a meth lab. What is missing from the records is the full story: The person is writing a novel about a character who makes meth. When he bought the books, he didn't consider how suspicious the purchase might appear to government officials, and his records didn't reveal the reason for the purchases. Should he have to worry about government scrutiny of all his purchases and actions? Should he have to be concerned that he'll wind up on a suspicious-persons list? Even if he isn't doing anything wrong, he may want to keep his records away from government officials who might make faulty inferences from them. He might not want to have to worry about how everything he does will be perceived by officials nervously monitoring for criminal activity. He might not want to have a computer flag him as suspicious because he has an unusual pattern of behavior.

The nothing-to-hide argument focuses on just one or two particular kinds of privacy problems—the disclosure of personal information

or surveillance—while ignoring the others. It assumes a particular view about what privacy entails, to the exclusion of other perspectives.

It is important to distinguish here between two ways of justifying a national-security program that demands access to personal information. The first way is not to recognize a problem. This is how the nothing-to-hide argument works—it denies even the existence of a problem. The second is to acknowledge the problems but contend that the benefits of the program outweigh the privacy sacrifice. The first justification influences the second, because the low value given to privacy is based upon a narrow view of the problem. And the key misunderstanding is that the nothing-to-hide argument views privacy in this troublingly particular, partial way.

Investigating the nothing-to-hide argument a little more deeply, we find that it looks for a singular and visceral kind of injury. Ironically, this underlying conception of injury is sometimes shared by those advocating for greater privacy protections. For example, the University of South Carolina law professor Ann Bartow argues that in order to have a real resonance, privacy problems must "negatively impact the lives of living, breathing human beings beyond simply provoking feelings of unease." She says that privacy needs more "dead bodies," and that privacy's "lack of blood and death, or at least of broken bones and buckets of money, distances privacy harms from other [types of harm]."

Bartow's objection is actually consistent with the nothing-to-hide argument. Those advancing the nothing-to-hide argument have in mind a particular kind of appalling privacy harm, one in which privacy is violated only when something deeply embarrassing or discrediting is revealed. Like Bartow, proponents of the nothing-to-hide argument demand a dead-bodies type of harm.

Bartow is certainly right that people respond much more strongly to blood and death than to more-abstract concerns. But if this is the standard to recognize a problem, then few privacy problems will be recognized. Privacy is not a horror movie, most privacy problems don't result in dead bodies, and demanding evidence of palpable harms will be difficult in many cases.

Privacy is often threatened not by a single egregious act but by the slow accretion of a series of relatively minor acts. In this respect, privacy problems resemble certain environmental harms, which occur over time through a series of small acts by different actors.

Although society is more likely to respond to a major oil spill, gradual pollution by a multitude of actors often creates worse problems.

Privacy is rarely lost in one fell swoop. It is usually eroded over time, little bits dissolving almost imperceptibly until we finally begin to notice how much is gone. When the government starts monitoring the phone numbers people call, many may shrug their shoulders and say, "Ah, it's just numbers, that's all." Then the government might start monitoring some phone calls. "It's just a few phone calls, nothing more." The government might install more video cameras in public places. "So what? Some more cameras watching in a few more places. No big deal." The increase in cameras might lead to a more elaborate network of video surveillance. Satellite surveillance might be added to help track people's movements. The government might start analyzing people's bank records. "It's just my deposits and some of the bills I pay—no problem." The government may then start combing through credit-card records, then expand to Internet-service providers' records, health records, employment records, and more. Each step may seem incremental, but after a while, the government will be watching and knowing everything about us.

"My life's an open book," people might say. "I've got nothing to hide." But now the government has large dossiers of everyone's activities, interests, reading habits, finances, and health. What if the government leaks the information to the public? What if the government mistakenly determines that based on your pattern of activities, you're likely to engage in a criminal act? What if it denies you the right to fly? What if the government thinks your financial transactions look odd—even if you've done nothing wrong—and freezes your accounts? What if the government doesn't protect your information with adequate security, and an identity thief obtains it and uses it to defraud you? Even if you have nothing to hide, the government can cause you a lot of harm.

"But the government doesn't want to hurt me," some might argue. In many cases, that's true, but the government can also harm people inadvertently, due to errors or carelessness.

When the nothing-to-hide argument is unpacked, and its underlying assumptions examined and challenged, we can see how it shifts the debate to its terms, then draws power from its unfair advantage. The nothing-to-hide argument speaks to some problems but not to others. It represents a singular and narrow way of conceiving of privacy, and

it wins by excluding consideration of the other problems often raised with government security measures. When engaged directly, the nothing-to-hide argument can ensnare, for it forces the debate to focus on its narrow understanding of privacy. But when confronted with the plurality of privacy problems implicated by government data collection and use beyond surveillance and disclosure, the nothing-to-hide argument, in the end, has nothing to say.

Daniel J. Solove is a professor of law at George Washington University. This essay is an excerpt from his new book, Nothing to Hide: The False Tradeoff Between Privacy and Security, published this month by Yale University Press.

If you have serious qualms with these practices the answer is easy - PAY for your e-mail and social sites.

13 people liked this. Like

1429523 2 months ago in reply to K

No one has to be "actually reading" anything. Say you type "bomb" and "plane" enough in your gmail. It's incredibly easy for gmail to filter for that content, analyze how often the words are being used in conjunction, and suddenly you're on a terrorist watch list.

I agree with your last bit though. I wonder if that would be a viable business model for a start up. "Pay for your email, and we won't look at it".

12 people liked this. Like

nali mikely 2 months ago in reply to 1429523

1429523 Yes, but then wouldn't it make sense to have terrorists just pay for the service and use it? Then what, make people go through a background check to join in?

7 people liked this. Like

Yang Yang Li 2 weeks ago in reply to 1429523

It's very simple to get your own email address. Use a fake email site that generates a email address for you. Or you can get your own server and install a email box on it. If you don't want to pay for the hosting and bandwidth fees, its easy to create your own server. Such as WampServer or Apache which turns your own computer into a server. For people not that tech savy, just download Opera which does the same thing automatically. You can trust Opera because it is run by Oracle, a security company.

That sounds like lots of work but it's not. Still want to have a private email account?

Like

cejaxon 2 months ago in reply to K

How do I pay? We aren't genuinely given that option -- where do you know of of a situation in which I can pay for a browser/email/search engine & free myself from tracking. I have a yahoo account, which came with my *buying* internet access from a large corporation. You could argue I already paid; in any event, I wasn't given the option of somehow paying more to opt out of privacy invasion.

It is true that Google is not good at identifying what people are really like -- for example, its data analysis in no way compensates for more than one person using the same computer. One of the largest users of my computer is my 10 year old daughter -- there's a site where you can find out how Google has classified you, & Google sees us as a middle aged *male*, despite my daughter's predilection for searching for Littlest Pet Shops.

To some extent this is part of a larger problem with businesses fetishizing metrics (which they do in numerous contexts that have nothing to do with privacy issues). You can measure lots of things, but the sum of those things doesn't give you a true picture. Often it gives you a distorted picture; in particular, it gives you a picture of what's easy to measure, not what's important to know.

10 people liked this. Like

mutualrespect37 2 months ago in reply to cejaxon

Based on reading Dr. Solove's column and all these wonderfully insightful comments, for the first time I just yesterday tried out the google chrome browser's incognito option. FoxFire offers similar, maybe even better options in this respect too, and there's a free browser and security suite called Tor that's highly recommended. I need to try reinstalling it. My first go a few weeks ago was not successful.

3 people liked this. Like

panacea 2 months ago in reply to K

I do pay for my email. And for my Web access.

It doesn't matter if they are reading it or not. The ads they bombard me with in response to using a service I PAY for are intrusive and annoying as hell.

11 people liked this. Like

LoboSolo 1 month ago in reply to K

You can also use GnuPGP to encrypt your email with online email if you use an app on your computer like Thunderbird to upload and download your email. Of course, the person on the other end must have your key to read it.

Like

glow_in_the_dark 2 months ago in reply to iris411

With all due respect - you gave your permission! Especially Facebook makes it possible for those who pay to gather data via 3rd party access - when you read the terms & conditions of most games on Facebook you will find that using the game doesn't just give permission to access your own data - it also permits access to your friends! The setting to prevent 3rd party access in such way is buried very, very deep in Facebook, and defaults to a free-for-all.

Until you as user set this, you are exposed via your friends.
Acoount - privacy settings - Apps & websites (below, left) - Turn off (and click through all the warning of damnation that will pop up). At least, that's what I would recommend..

13 people liked this. Like

Dave 2 months ago in reply to glow_in_the_dark

Actually, Facebook has a terrible reputation for bad management of private data. Even with their private settings are turned on, people can still access data on your account through a variety of methods

8 people liked this. Like

Dave 2 months ago in reply to iris411

Download a copy of firefox and try out some of the cookie management plugins listed at http://mashable.com/2008/11/11..., you can use that to block a fairly large proportion of the tracking done by companies like facebook and google for advertisement. Facebook is probably more of a risk, as accounts with them can and are used to access a range of sites (twitter too, seeing as I'm using a twitter account to make this comment) and so can tie activities to a single user. If you keep separate

accounts for separates sites though or make sure to log out of your account when done (even if you use it to access a different site) you can limit the data which can be tracked

Alternatively, both firefox and chrome have private browsing which negates most of the tracking methods used online (although again, the use of accounts on multiple sites is still an issue)

6 people liked this. Like

mccaugheym 2 months ago

If you want to read how Solove's argument plays out specifically for those of us in the academic profession, read how the police at my former university seized and searched my computer, without a warrant, and how the university administration (and many of my colleagues) rationalized it. And, my 2003 article mentions both Orwell and Kafka. Many did insist that I should not mind the seizure, search, and copying of all the records on my state-issued computer harddrive "if I had nothing to hide." I argued then, and still argue, that it's not about hiding something. Professors have to be protected from unwarranted searches by government officials, including the police, so that we can do our work with academic freedom. Academic freedom enables us to create scholarship that is not hidden but ultimately benefits the public. See the short essay in Academe online at:
http://www.aaup.org/AAUP/pubsr...

56 people liked this. Like

wingedwarrior 2 months ago

-I'm not ashamed that I use the bathroom, but I don't want to be watched.
-I've not kept dirty magazines in my underwear drawer since I was a boy, but you I don't want people going through it.
-Even legitimate information can be used for illegitimate purposes.
-Do I STILL cheat on my taxes? Well, uhhhhhh...

13 people liked this. Like

Abu Nudnik 2 months ago

"Privacy, in other words, involves so many things that it is impossible
to reduce them all to one simple idea. And we need not do so."

It is certainly possible and we need to do so. The distinction between private and public is simple and clear. The same arguments against CCTV cameras are now been used in England to bash street photographers over the head.

When people complain about my passion, street photography, saying they have a right to privacy I tell them they certainly do: "Close your door and you're in private. You're in public now."

5 people liked this. Like

mutualrespect37 2 months ago in reply to Abu Nudnik

Professor Solove's article does not make complete sense without an understanding of his "taxonomy of privacy," which he does not include here:
Information CollectionSurveillanceInterrogationInformation ProcessingAggregationIdentificationInsecuritySecondary UseExclusionInformation DisseminationBreach of ConfidentialityDisclosureExposureIncreased AccessibilityBlackmailAppropriationDistortionInvasionIntrusionDecisional Interference

He thus defines privacy as a family of resemblances based on the above categories, not as an essence.(From "Why Privacy Matters," 2008)

Professor Solove does not define privacy by a simple public/private opposition either. Instead, he claims it is in society's interest to give individuals the freedom to flourish rather than inhibiting them and chilling their expression and spontaneity of action through constant surveillance and intrusion.

For me, respecting privacy is fundamental to equal opportunity in the schools and workplace. If you are a photographer, Abu, it certainly would be respectful to ask permission before photographing people. People should not have to stay indoors just to avoid harassment on the basis of their variance from the white, male, mainstream template of the individual or simply for being who they are. This interferes with people's right to freedom of movement.

A few years ago, I was placed in a unjust situation where the campus cops showed up at my residence to collect affirmative action data from me. There is a privacy and civil rights law that precludes colleges from requesting or demanding such information before admission, and a good-faith police officer would have honored that. In this case respecting my privacy involved treating me like anyone else, not subjecting me to police harassment on the basis of perceived difference. Homogeneous places like NE and KS seem to have a hard time wrapping their heads around the idea and importance of privacy though.

6 people liked this. Like

mutualrespect37 2 months ago in reply to mutualrespect37

The text box above did not save my formatting but the main categories should be 1) information collection 2) information processing 3) information dissemination, and 4) invasion.

Like

Abu Nudnik 2 months ago in reply to mutualrespect37

It would respectful of me to ask permission to take photographs in the street but candid street photography would disappear entirely. By the time I went to ask everyone in the street for permission, the scene I had found interesting (sometimes just relations of color and shapes) would long ago have been gone. What about my pursuit of happiness? my freedom in public? my freedom to, without harm, engage in my passion? my documentation of the world as I see it for posterity? How does the future have a real glimpse of real people, long gone, without this invaluable candid recording?

It would be respectful of people not to use foul language, not to stand in the stairwells of buses, not to take up two seats on the subway, not to spit on the sidewalk, not to talk constantly on cell phones, push by you on the sidewalk.... but they do.

Without candid street photography, governments and their CCTVs would have a monopoly on public scrutiny. Who watches the watchers? Street photographers. Street photographers have provided evidence in cases, for instance, of police brutality and other crimes.

I like to use the adultery standard. If a man and woman engaging in an adulterous affair are caught smooching in the street by their husband and wife, would they have a "right" to "privacy?" The notion is absurd. As is the one that says a photographer can ruin a marriage by outing an affair. This would only be true if the photographer forced the couple to marry, forced them into adultery and forced them to be at just that particular park bench to snap the photo.

As for this sentence, I am at a loss: "People should not have to stay indoors just to avoid harassment on the basis of their variance from the white, male, mainstream template of the individual or simply for being who they are." Who would photograph people in the street for such a variance? Not I.

5 people liked this. Like

mutualrespect37 2 months ago in reply to Abu Nudnik

Right now, I am living in a backwoods situation where I get aggressively approached by strangers, and from my perspective harassed, nearly every time I try to use public space. The remark about being bothered on the basis of diverse characteristics was thus not aimed at you. Apparently people in this area of the country are mindlessly trained up to behave like this, but not respecting decent social boundaries does result in people getting too personal and alienating others with privacy violations. Government employees can be legally challenged for behaving this way , but with private individuals I'm not sure much can be done. If one fails to receive the gesture as friendly these unsophisticated types will often

quickly turn abusive. I much prefer the areas of country I have previously resided where it is considered a civic virtue to mind one's own business in public unless someone is truly in an emergency or you obviously share an interest in common. Women are starting to organize to protest "street harassment," and what I've recently faced is a version of this. This spring the first annual anti-street harassment day was celebrated.

Good luck with your photography! I'm sure you are doing a form of community service(even though some of us do not appreciate being photographed).

5 people liked this. Like

cust0s 1 month ago in reply to Abu Nudnik

Oh Abu!

I would caution you to be careful. I love photography as much as the next one but my sentiments and that of my wife close resemble Mutual Respect's feelings. I'm not sure what your background is but just because you're in public does not give you the right to snap photos of just anyone here and there. Depending on what the photo implies, the age of the person photographed, and what you do with said photo you might be opening yourself up for a lawsuit of "false light," "defamation," and other laws protecting the photographing of minors. I could go into various examples, but I just don't have the time today. However, you could easily research a few on your own. Your best bet is to just get permission and there are no problems because you obtained consent and assent. Again, I love photography too, but others I know who used my image learned this the hard way. I did go to law school and I knew my rights.

Cheers and good luck with a fun hobby.

Like

Antsy Kuhnwisse 2 months ago in reply to Abu Nudnik

If only there were some opt-out provision, some universal symbol for "Please don't take my photo" that one could display, so photographers would have a way to avoid certain people without (hopefully) losing the "moment."

Why do I not want my photo taken? Maybe I don't like the way I look in photographs. Maybe I invariably show up with a stupid look on my face, or in a goofy pose. Or maybe that's not it at all. I just hate it. Being photographed without my consent feels like an assault to me.

13 people liked this. Like

mutualrespect37 2 months ago in reply to Antsy Kuhnwisse

I appreciate your courage in stating this view, Antsy. Personally, I do not like being photographed or treated like a physical object by those blind to spirit and intellect either. I too need to wear "Stand back" or "Back off" t-shirt in these sophisticated parts of the country. Often going beyond mere speech and verbal privacy violations such street harassment behavior involves actual physical touching, and strangers manhandling one's belongings.
Although I'm from the West Coast the part of the country where I have moved to teach has a widespread social norm that allows complete strangers to self-flatteringly present themselves as Good Samaritans and approach strangers in this role at will. The problem is that this is often done on the basis of offensive stereotypes-- to pregnant women or someone using a white cane, for instance. It's all about pigeon-holing people based on first impression and taking a patronizing"You look like you need help" attitude. There are definite safety issues involved, first of all. Even if "help" were welcome, few people these days can afford to trust a stranger. Twice, in two neighboring states, I have recently been brutally blamed for and subject to police and criminal injustice harassment for letting such offensive, kiss-to-kill types know they need to mind their own business. I have had cruel, blame-the-victim smears placed against me.How dare these mindless, presumptuous, people invade decent social boundaries and terrorize complete strangers? It ends up that behavior like this can and does affect equal rights to work and education. It involves bigotry and prejudice.

Parents in the South and rural states like MO and KS train up their kids to behave like this. It

appears to substitute for any truly reflective code of ethics-- as a drama they play out in public to add up points for entrance into heaven. It's a tautology--I say I'm helping so dare you be ungrateful? My sanity has always been predicated through keeping decent boundaries and the ability to choose my friends, so this system seems barbaric to me. It's ruining my life and ability to enjoy public space.

6 people liked this. Like

iquanyin moon 2 months ago in reply to mutualrespect37

well, i trust most strangers. and its been just fine. taking a photo /is not harming anyone nor taking anything from them./ period. theres no safety risk. none. as to stereotypes, maybe and maybe not. in a given situation, you're not a mindreader and you don't have to be. people who take photos are //into an art form/ and its /not about you/ and oh yes... in one sense, yes, we are objects, in that we are creatures who occupy space. we have physical attributes. eyes see us, painters paint us, writers write about us, actors portray us, and so on. please people, stop trying make artists somehow guilty of something.

its a weird attitude and a sign of the fear culture we have here in this country that people are protecting...um, nothing at all. from artists. artists do art.

what's nest, no one can look at anyone in a cafe and then write in their notebook because they might be writing about ... people in the cafe?

1 person liked this. Like

12080243 2 months ago

At usmnews.net, here is just one of our daily government visitors (not weekends, of course):

Mississippi, Department Of Information Technology (69.60.33.244) [Label IP Address]

Ridgeland, Mississippi, United States, 80 returning visits

DateTimeTypeWebPage16th May 201116:13:21Page ViewNo referring linkwww.usmnews.net/

Like

Mick Jagger 2 months ago

This has got to change before we have a world not worth having.

10 people liked this. Like

willismg 2 months ago

It's not about what I may or may not have done wrong, it's about what the government may or may not do wrong with the information.

31 people liked this. Like

12080243 2 months ago

Here's today's government visitor to www.usmnews.net (they don't visit on the weekends):

Mississippi, Department Of Information Technology (205.144.229.19) [Label IP Address]

Jackson, Mississippi, United States, 288 returning visits

DateTimeTypeWebPage17th May 201107:15:35Page ViewNo referring linkwww.usmnews.net/

Like

snihighereducation 2 months ago

Great article, spot-on. In the less extreme, the 'nothing to hide' argument is challenging but this excerpt does a great job addressing that.

5 people liked this. Like

PEZ 2 months ago

It's impossible to know if you have something to hide or not. The Government can change the laws or change the interpretation of them at any time. And they will.

19 people liked this. Like

mutualrespect37 2 months ago in reply to PEZ

Prof Solove makes the point we do not know how our information will be used: we can't predict that, which is basically what you are saying, PEZ. Plus, our information can be aggregated. Information that isn't harmful alone may become so when combined with other data.

4 people liked this. Like

11299051 2 months ago

Perhaps with all the data available about Internet, banking system, and other users we may all eventually be metamorphized into virtual bugs in the eyes of the Government. Now when I look at an Internet site with an eye to purchasing an item I am subsequently inundated with ads from that company for days or weeks as if no other merchant might ever interest me. For the present I eschew Internet purchases and the use of credit cards. Guess how much money I'm saving and how much much my peace of mind has improved?

2 people liked this. Like

walkerst 2 months ago

I can think of a number of situations in which an individual has nothing dreadful to hide, but certainly has things they don't want everyone knowing. For example, if you have a mental illness such as mild depression, and you take medication for it. Do you really want this to be public? In many cases, I suspect the answer would be no. Mental illness still carries a strong stigma. You may function perfectly, but others may treat you as if you are less capable or reliable. Worse still, I can think of a situation that has happened to me personally - a stalker. Unfortunately, said nutcase was also a computer genius. Do I want surveillance photos of me - or any photos of me - in databases? Certainly not. There are some out there, but I have refused to have them posted wherever possible. I have changed my name to something extremely common, left my home country, changed my profession, and taken many more precautions. The psycho found me a number of times, but I've at long last gotten rid of the jerk, I think, and I'm starting to relax. But the more data there is about you that someone can potentially access, the more likely it is that a stalker can find you. That's one instance where I have nothing to hide, but certainly don't want tons of information about me hanging around where a smart computer geek can get it. Privacy in some instances can be a matter of life or death.

20 people liked this. Like

delfeld 2 months ago

Excellent article!

I like to think of the hardest (common) logic problem is the problem of modus ponens (if-then). If p then q does not say anything about q if not p . . . it *only* says something about q *if* p. From this, this MP argument is the result of a false use of modus tollens (not q, so not p):

1. (MP) If "did something wrong", then "hides (access)".
2. (MT) Assume not "hides". Then not "did something wrong".
3. (False logic!) Therefore, if not "did something wrong", then not "hides".

It is hard to convince through logic, though. So digging into the heart of the "truthiness" of the claims is equally effective at destroying this false accusation. Showing how this argument reduces the collection and use of information to 'nothing to
worry about' nails it. It is nice to see it so
well stated.

4 people liked this. Like

glow_in_the_dark 2 months ago

May I be so bold to add a few thoughts to this rather excellent article?
First of all, I would like to point out that the key concept of "1984" was actually developed in 1785 by the English philosopher and social theorist Jeremy Bentham. It was a prison concept called the "Panopticon", a design aimed at making inmates feel they were *always* under observation. Personally, I find that original concept disconcertingly apparent in places like London, UK with its excessive CCTV coverage. As a slight digression I would add to this situation a question attributed to the Roman poet Juvenal as found in his "Satires": "Quis custodiet ipsos custodes?" (Who watches the watchmen?).

Secondly, we need to distinguish between rights and privilege. Privacy is a Human Right (#12) - you are born with it. The State has to exercise its function of managing society (a structure partially defined by laws), and is thus granted the PRIVILEGE to break privacy in a defined set of circumstances. It is by not means a right - it is a privilege as it allows an exception to rights to exist for very specific reasons. When those conditions no longer exists, the privilege vanishes with them.

Thirdly, a common mistake made by the end users of data aggregation is to consider the result of an aggregation a fact. It never is - it is a PROBABILITY. This is also the dirty little secret of biometrics such as fingerprints: they establish PROBABLE matches - not absolutes. The difference between facts and probability are simply not understood by those who receive the end product of such aggregation, and many problems occur as a consequence. If the TSA profiles someone as "worthy of further investigation", the relevant agents must be briefed that such a flag is merely a probability and could be wrong.

Kind regards, GitD

12 people liked this. Like

glow_in_the_dark 2 months ago

Duplicate comment removed.

(Edited by a moderator)

2 people liked this. Like

Antsy Kuhnwisse 2 months ago in reply to glow_in_the_dark

To what does "(#12)" refer? In what sense are we "born with" privacy or the right to it, when infancy is clearly the time of the least privacy most humans will ever have?

2 people liked this. Like

glow_in_the_dark 2 months ago in reply to Antsy Kuhnwisse

Maybe worth catching up on some history at http://www.un.org/en/documents.... I'll copy the header of that page below, after that I suggest you read article #12.

On December 10, 1948 the General Assembly of the United Nations adopted and proclaimed the Universal Declaration of Human Rights the full text of which appears in the following pages. Following this historic act the Assembly called upon all Member countries to publicize the text of the Declaration and "to cause it to be disseminated, displayed, read and expounded principally in schools and other educational institutions, without distinction based on the political status of countries or territories."

4 people liked this. Like

Antsy Kuhnwisse 2 months ago in reply to glow_in_the_dark

I appreciate the response and the link. I'm aware of the U.N. Declaration -- just not so extremely versed that I instantly recognize a reference to "#12". Thought it might be helpful to others, too, to spell out what you're talking about, rather than assuming all possess the same knowledge you do.

3 people liked this. Like

greeneyeshade 2 months ago

I wonder a bit about the rights and privileges of investigators--not always the government by the way; you're own university can look at all your emails if they wish--and what their limits are if there is credible probable cause that something seriously illegal is going on. Email is a personal thing; the investigators will see considerable information that's irrelevant to whatever they are looking for, and if a person truly is dishonest, they may discover wrongdoing beyond what they had imagined and unrelated to the things they were searching for. I suppose one has to say that one forfeits one's rights to privacy once a certain line has been crossed, but it seems to me that investigators should take care to keep only relevant evidence.

Like

Load more comments