

# Comments to the Federal Trade Commission on the Informational Injury Workshop and P175413

January 22, 2018

I am an independent privacy consultant with the boutique firm Enterprivacy Consulting Group, primarily focused on Privacy by Design (or “Data Protection by Design and Default” for my clients working under Article 25 of the EU General Data Protection Regulation). The focus of the consultancy is on providing training, program development and subject matter expertise on building privacy considerations into products, services and processes. This includes training clients on the consequences of privacy violations on individuals. Privacy is a rapidly evolving field and I am constantly absorbing new information to improve the services I provide clients so I appreciate the opportunity to learn from the FTC’s workshop as well as provide these comments.

I am a licensed attorney in the state of Florida, having attended Florida State University with the specific intent of getting into privacy law. Further, I am a Certified Information Privacy Professional (CIPP/US), a Certified Information Privacy Manager (CIPM), a Certified Information Privacy Technologist (CIPT) and a Fellow of Information Privacy with the International Association of Privacy Professionals. Back when the Information and Privacy Commissioner's office in Ontario Canada was still designating such, I was designated a Privacy by Design Ambassador for my work in promoting privacy by design. I’ve written, lectured, and spoken professionally on the topic. I’ve been involved in privacy and information security since 2004 though my personal interest precedes this to the days when my house-mate was a private investigator and repossession agent and I realized the wealth of information about individuals that were veiled from public knowledge.

Though I wasn’t able to attend in person, I enjoyed spending the day watching the FTC workshop on Informational Injury on December 12<sup>th</sup>, 2017. I am in the fortunate position of submitting my comments after the workshop and thus am able to benefit from the insights and discussions that occurred during the workshop as well as the written comments submitted by others.

I wanted to address, in detail, two misconceptions that I saw portrayed at the workshop and in some comments. Both relate to whether a privacy harm must be particularized and actualized to warrant regulatory action and intervention. Specifically, the first misconception I will address is whether the risk of a privacy violation is harm enough to warrant regulator action. The second is whether a privacy violation which results in no harm still constitutes a violation.

## Risks of Privacy Harms

Automobile accidents in the United States killed over 37,000 people in 2016. Nearly 2.5 million people were injured.<sup>1</sup> Billions of dollars are spent every year repairing property damage due to car accidents. When an accident occurs, litigation can result to determine not only the proportional fault of the parties to the accident but also a distribution of compensatory remedies. In order to reduce the transactional costs of litigation on all parties, insurance companies and personal injury attorneys have fairly common industry practices to assess liability. Typically, only edge cases go to court and many of these still settle before trial. This all occurs after an accident occurs and injury and property damage results. Even given the scale of effects mentioned above, it’s relatively

---

<sup>1</sup> Rocky Mountain Insurance Information Association, *Cost of Crashes and Statistics*, available at [http://www.rmiia.org/auto/traffic\\_safety/Cost\\_of\\_crashes.asp](http://www.rmiia.org/auto/traffic_safety/Cost_of_crashes.asp)

small compared to the 300+ million people in the United States and estimated 3 trillion miles driven per year. By comparison, approximately 600,000 people die of heart disease every year in the US.<sup>2</sup>

Speed is one of the factors contributing to injury and damage in auto accidents. The velocity of a vehicle has a causal effect on both the likelihood of an accident and the severity of the resulting injuries and damage. Only a fraction of automobile trips result in an accident. In aggregate, however, the social costs are readily apparent. When Congress repealed the National Maximum Speed Limit law in the 1990s, there was a rise in mortality evidenced.<sup>3</sup> Having a population of drivers increase their speed resulted in a measurable increase in accidents, injury and damage.

If every-time I drove over 55mph I caused an accident and killed a pedestrian and ended up being held liable in court, not only would I quickly learn not to drive fast but I'd probably be able to learn from observing others and never do so in the first place. But, because of the rarity of accidents, there exists a disconnect, in the minds of drivers, between driver behavior (speeding) and the resulting social harm. Not that drivers are unaware that speeding increases accidents and damage, just that link is not sufficiently direct enough to govern their behavior. Courtroom liability is also an insufficient deterrent to risky behavior because of this disconnect as well.<sup>4</sup> There are potentially biological reason why humans are better at dealing with immediate risks (being attacked by a lion in front of us) than future ones (cancer from smoking).

The risk to a speeding driver may be small on a daily basis to any one driver but the aggregate risk to society of all drivers speeding for a year are measurable and consequential. There exists means to lessen this aggregate harm of speeding, many of which shorten the time between a driver and negative consequences they face of speeding, thus incentivizing them to reduce their speed, resulting in aggregate social benefit. Speeding tickets are issued to more drivers and have a smaller take on their pocket book than an accident would but the combined likelihood and impact (the measure of risk) are on par with an accident (smaller impact, higher likelihood for ticket versus smaller likelihood, higher impact for an accident). But that increased likelihood creates a much stronger causal link in driver's minds between speeding and adverse consequences (getting pulled over).<sup>5</sup> And while a court may award damages in the case of an actual accident, judges in traffic court don't assess the fine based on damages. The fines are statutorily set to manage the behavior of drivers and reduce accidents and consequences across society.

## What about privacy?

Like speeding, privacy violations can cause harms which can be far off in the future and only have a discernible impact in aggregate. An identity thief may find personal data on a discarded copier hard drive in a county landfill years after the victim gave it over to the auto dealer to process his or her credit application. This time difference produces the same effects as the distant accident for speeders, it is insufficient to regulate the victim's behavior when they handed over personal information. And while one might think companies are more rational actors, because of their profit motive, they too suffer a bias toward present profits over future risks. Additionally, companies may rely on insurance to offset future risk, though most insurance policies are woefully inadequate in this regard (capping awards, excluding cyber-security incidents, etc..) leaving most companies under-insured. An over reliance on inadequate insurance means companies engage in riskier behavior than they are internalizing the costs for.

---

2 Centers for Disease Control and Prevention, *Deaths and Statistics (2016)*, available at <https://www.cdc.gov/nchs/fastats/deaths.htm>

3 Insurance Institute for Highway Safety, *Deaths go up on interstate highways where higher speed limits are posted (2009)*, available at <http://www.iihs.org/externaldata/srdata/docs/sr3401.pdf#page=4>

4 The disconnect is referred to as hyperbolic discounting. We discount the future costs of injury and damage for present benefit (getting where we need to be quicker by speeding).

5 The somewhat tongue-in-cheek proposed "Tulloch Spike" which placed a spike in the middle of the steering wheel aimed at the driver was another example of viscerally and immediately reminding people of the risks they are imposing on others through careless driving. The Tulloch Spike was primarily aimed at countering driver safety initiatives by demonstrating the need to internalize to drivers their externally imposed risk on other automobiles and pedestrians. See <https://jalopnik.com/theres-actually-a-name-for-a-steering-wheel-with-a-big-1791445206>

There are three other problems that make court remedies insufficient to handle consequential

1. **Many of the injuries resulting from privacy violations are not cognizable in court.** - First and foremost, courts are reluctant to provide a remedy where the damage is psychological, such as embarrassment, anxiety or altered behavior. Further, courts would be hard pressed to recognize some objective harms, such as a human rights worker being incarcerated in a foreign prison as a result of disclosure of their emails by their US based ISP. Even some monetary impacts may be too tenuous for courts to acknowledge. This is in contrast to auto accidents where property damage is easily quantified and even personal injury can generally be measured and compensated (though remedying soft tissue injury might not be so easily quantified).
2. **Harms may not be traceable by victims.** - Many victims of identity theft couldn't tell you how the thief got their personal information. Enterprivacy Consulting Group's current intern relayed a story from her home country in Central America where people were being blackmailed with their personal information, because, as it turns out, the blackmailers had posed as sweepstakes companies and tricked individuals into revealing personal information. The blackmail calls came months later, making it difficult for victims to make the connection of how the blackmailers got their personal information. This akin to a pedestrian involved in a hit and run, they know they were injured but not by whom and unlike other drivers who have no-fault insurance or uninsured motorist coverage, pedestrians may have nowhere to turn to recoup the costs of their injuries. Similarly, victims of privacy violations often have little recourse.
3. **Harms may not be realized by victims** – Some harms of privacy violations may never be realized by the victims. Job candidates may never know that they didn't receive a call back from a hiring manager because of what the hiring manager found through a social media search of the candidate's phone number. Homeowners may never know that they didn't receive a mortgage modification offer with a low rate (which others did) because they frequently shopped at a discount store using their credit card. If a pedestrian is hit by a speeding car, they know it. Not all victims of privacy violations are aware they are victims.

Similar to traffic laws that seek to reduce the societal risk of speeding and other risky driver behavior, regulations can reduce risky behavior around privacy violations. Relying on only post-harm enforcement does nothing to eliminate the discounting of future risks, the non-cognizable injuries, the harms that lack traceability to a specific actor or harms that victims may not be aware of.

## Violations without harms

Professor Ryan Calo does an excellent job of delineating privacy harms in his paper *The Boundaries of Privacy Harm (2011)*, but admits that violations and harms exhibited a disconnected relationship. One can clearly have harms without violations (something Calo's notion of perception captures "the belief that one is being monitored"), so why not violations without harm? What if a doctor, whose Hippocratic Oath imposes a duty of confidentiality, discloses a patient's ailments to her friends on Facebook? Even if the patient never knows about it (no subjective harms) and suffer no ill effects (no objective harms), the breaking of that duty is a violation of the trust the patient placed in the doctor. Confidentiality is foundational to the sharing of information in the doctor/patient relationship, and their sharing of information was predicated on the doctor's duty and responsibility to them. From our third party vantage, even though the patient isn't aware, there seems something instinctively wrong with the doctor's actions, a violation of trust has occurred.

Consider a more visceral example. If someone (aka Peeping Tom<sup>6</sup>) were to place a camera in your shower, you no doubt would consider that a “violation of your privacy.” But what exactly are the effects, on you, of that violation? If you knew about the camera, in advance, you might alter your behavior, rarely showering or showering only in cutoff jeans.<sup>7</sup> This would certainly be an inconvenience. You might feel embarrassed, distressed, or, in extreme cases, suffer anxiety as a result. After the fact notification that there had been a camera in your shower would also likely result in these mental or psychological effects, only delayed.<sup>8</sup> But what if you didn’t know? What if you never knew?

Harms are predicated on knowledge of the violation by either the victim or others and that results in some measurable effect on the victim of the violation. Even just to have members of society alter their perception of the victim is measurable by asking those members how they feel about the individual. But what if the perpetrator never shares his surveillance footage and his relationship with the victim is so far removed and his mental state is such that any alteration in perception is negligible (in the scope of the entire world). What if the surveillance footage were mangled or the camera failed to function? We still see this act by the perpetrator of putting a camera in your shower as a “violation” of privacy. Even if the actions are never discovered, the mere act is unconscionably invasive; the victim’s sanctity must be inviolate. Acts of these types are still something society wishes to prevent.

Both the doctor and the Peeping Tom exhibit a form of inequality between the violator and the violated. The violators know something the victim does not (the violator’s intended or eventual use of the information). The violators took advantage of their access to information, which but for the victim’s lack of knowledge, the victim might have taken action to prevent. The interactions seem very one-sided, the benefit befalling the violator with no benefit on the violated; the relationship is asymmetric. From a purely economic social welfare analysis perspective, society is better off, society is ‘happier.’ You, and the patient, are no worse off, because both are unaware and suffered no objective consequences. Tom, in his peeping, is happier because of his illicit watching. The doctor, and her friends, are happier (debatably) from discussing your ailments. So society, on net, is now happier as a result. But you still probably think that we shouldn’t encourage Peeping Tom’s behavior, despite his increased happiness and your unawareness. Why? Is it the prurient nature of Tom’s behavior? What about the doctor?

Consider two college roommates. One, believing the other is stealing food from him, places a hidden security camera in the dorm room. He comes to find out, not only is the roommate not stealing, but a mouse is doing it. He does discover that the roommate is skipping class and doing drugs frequently. Not wanting to reveal his surveillance to the roommate, he quietly seals the mouse hole and never tells the roommate or anyone else. A privacy violation has occurred but no consequences have befallen the observed roommate. Social welfare has increased, as the suspicious roommate is happier, having had his suspicions alleviated, no longer is losing his food to the mouse, and the suspected roommate is none the wiser (in other words he isn’t ‘less happy’). In fact, the suspicious roommate may now be treating the previously suspected roommate better because of his increased trust and the suspected roommate now enjoys no longer having a mouse invade his dorm room as well, so the violation resulted in a benefit to the suspected roommate too. Yet, we still have the problem of a privacy violation occurring. We don’t, as a society, want to encourage this behavior (covertly monitoring roommates), do we?

One could argue that absent actual harm what is sought is preventing of the risk of harm. In other words, our covertly monitored roommate could be discovered as the thief and be expelled, he could find the camera and be embarrassed, the footage could be stolen and result in subsequent use

---

6 Colloquially a Peeping Tom is a male archetype who leers at women in states of undress, typically in places they expect privacy.

7 A fake psychological condition, in which the afflicted party can never be fully nude, not even alone, turned cultural meme by the TV show *Arrested Development*. <https://www.urbandictionary.com/define.php?term=nevernude>

8 In 2008, sportscaster and TV personality Erin Andrews was filmed nude in a hotel room. She didn’t learn about it until late when video footage appeared on the Internet.

that results in one or another consequence to him (expulsion for drug use). While true, the invasiveness of the suspicious roommate's action aren't based on some analysis of the risk of secondary consequences, but rather that the act, regardless of consequences, regardless of the risk of consequences, regardless of the benefits is reprehensible to society's sense of right and wrong. The inequality in the relationship, the violation of trust and norms is what drives our dislike the behavior. Thus, in any analysis of privacy violations, the absence of consequences on the violated should not be presumptively exculpatory on the violator. We should seek to prevent violations, not harms.

Thank you for your time and this opportunity to comment.

R. Jason Cronk

Privacy and Trust Engineer

Enterprivacy Consulting Group

<https://enterprivacy.com>