ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

October 27, 2017

Federal Trade Commission
Office of the Secretary
400 7th Street, SW, Suite 5610 (Annex A)
Washington, DC 20580

RE: Informational Injury Workshop, Project No. 175413

To Whom It May Concern,

The Information Technology and Innovation Foundation (ITIF) is pleased to submit these comments in response to the Federal Trade Commission's (FTC) request for comment (RFC) on its workshop to explore issues relating to consumer informational injury in the context of privacy and data security.[1] ITIF is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation, and pro-technology public policy agenda that spurs growth, prosperity, and progress. ITIF supports the FTC's decision to host a workshop exploring how consumers may suffer injuries when information about them is misused.

The FTC has shown leadership on privacy and data security issues, bringing over 170 cases against many entities for committing unfair, deceptive, or fraudulent practices in 2016.[2] The FTC's efforts around privacy and security have often centered around protecting "personally-identifiable information" (PII) or "personal data," terms that can apply to all information that can be reasonably linked to an individual, computer, or device.[3] PII can include a wide range of information, from names and email addresses to personal photos and

[1] "FTC to Host Workshop on Informational Injury; Seeking Public Comments," *Federal Trade Commission*, accessed October 24, 2017, https://www.ftc.gov/system/files/attachments/press-releases/ftc-announces-workshop-informational-injury/public_notice_injury_workshop.pdf.
[2] "Privacy and Data Security Update (2016)," *Federal Trade Commission*, January 2017, accessed October 24, 2017, https://www.ftc.gov/reports/privacy-data-security-update-2016
[3] Jessica Rich, "Keeping Up With the Online Advertising Industry," *Federal Trade Commission*, April 21, 2016, accessed October 24, 2017, https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry; "Protecting Consumer Privacy in an Era of Rapid Change," *Federal Trade Commission*, March 2012, accessed October 24, 2017, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

IP addresses.[4] Indeed, the definition of PII varies across federal agencies, between federal and state government, and across different countries, and the definitions have continued to change to include different forms of data that would previously be considered "non-PII" over the last decade.[5]

However, not all PII is the same. A better understanding of the different types of PII would help the FTC accurately identify consumer harms associated with each type of information and intervene more effectively while not impeding innovation. The purpose of these comments is to propose a typology for types of PII, informational injuries, and levels of data collection and use to help the FTC achieve this goal. Moreover, as we outline below, the conventional wisdom that restricting data sharing is the optimal way to prevent informational injury in most cases is simply incorrect. A more nuanced approached to preventing informational injury will allow the FTC to pursue better alternatives depending on the type of information at risk.

TYPES OF PII

PII is information that can be used to distinguish or identify an individual or can be linked or is reasonably linkable to that individual.[6] There are four major categories of PII, each with different levels of inherent privacy interest.

The first category is **observable information**, which is personal information that can be perceived first-hand by other individuals. This category includes both observable personal information created by the individual about him or herself, as well as observable personal information captured by a third party. An example of the former is personal correspondence, such as letters or emails that a person has written. Examples of the latter primarily come from recorded media, such as video surveillance (e.g., CCTV camera footage), photographs

[4] "Website Operator Banned from the 'Revenge Porn' Business After FTC Charges He Unfairly Posted Nude Photos," Federal Trade Commission, January 29, 2015, accessed October 24, 2017, https://www.ftc.gov/news-events/press-releases/2015/01/website-operator-banned-revenge-porn-business-after-ftc-charges.

[5] William Baker, "The Changing Meaning of 'Personal Data'," *Wiley Rein LLP*, March 22, 2011, accessed October 24, 2017, https://www.lexology.com/library/detail.aspx?g=7f27f25f-0076-4ec0-86ac-7cf81c5a62d1.

[6] We pulled this definition from several sources, including Erika McCallister, Tim Grance, and Karen Scarfone, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," *National Institute of Standards and Technology*, 2010, accessed October 24, 2017, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf; The Privacy Act of 1974, 5 U.S.C. § 552a; and "Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission Before the Federal Communications Commission," *Federal Trade Commission*, May 27, 2016, accessed October 24, 2017, https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf.

(e.g., personal photos), or audio recordings (e.g., recording of a conversation). Media captures personal data in a way that, while recorded by a third party, any individual can observe it for themselves by looking at the photo, watching the video, or listening to the recording. Observable information can have important privacy implications for individuals.

The second category of information is **observed information**, which is information collected about an individual based on a third party's observation or provided by the individual, but does not allow someone else to replicate the observation. This data can encompass a wide variety of information that describes an individual, such as their basic information (e.g., place of birth, date of birth, etc.), physical traits (e.g., weight, eye color, etc.), personal preferences (e.g., likes and dislikes, political views, search history, reading habits, media consumption, etc.), social traits (e.g., degrees, religious affiliations, nationality, criminal history, etc.), family information (e.g., marital status, child information, etc.), employment information (e.g. job history, salary, etc.), biological conditions (e.g., sexual orientation, medical conditions, medical lab results, disability information, etc.), and geolocation information. Information in this category can have privacy implications for some individuals, but it can also be used and analyzed to create value.

The third type of information is **computed information**, which is information inferred or derived from observable or observed information.[7] Computed information is produced when observable or observed information is manipulated through computation to produce new information that describes an individual in some way. For example, companies construct online advertising profiles for consumers based on many different sources of observed information, such as direct-mail responses, search history, and demographic information. Or some companies use algorithms to analyze video feeds to count how many people walk past a certain location. Similarly, biometrics are derived through a computational process from scans of unique physical characteristics on a person's body. For example, the Transportation Security Agency (TSA) uses backscatter x-ray machines to scan individuals' bodies during security screenings at airports to generate a generic outline of a human body with areas containing potential contraband highlighted in the image.[8] Information in this category is primarily used to create value for the organizations that computed the

[7] The definitions we use in this report for "observed information" and "computed information" are similar to the ones the Article 29 Working Group has used for "observed data" and "inferred data." See Article 29 Data Protection Working Party, "Guidelines on the right to data portability," December 13, 2016, revised April 5 2017, 10, https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf,.

[8] Transportation Security Administration, "TSA completes installation of state-of-the-art checkpoint screening equipment at six Minnesota airports," *news release,* June 8, 2017, accessed October 24, 2017, https://www.tsa.gov/news/releases/2017/06/08/tsa-completes-installation-state-art-checkpoint-screening-equipment-six.

information, and often has fewer privacy implications for individuals. However, computed information may be generated from multiple sets of data and combined to give a "mosaic" picture of an individual's life.[9]

Finally, **associated information** is information that a third party associates with an individual. Associated information, by itself and unlike the other three categories, does not provide any descriptive information about an individual (i.e. it does not describe qualities about an individual). For example, a library card number alone does not provide any information about its owner. (Someone may be able to infer information about an individual based on the fact that he or she has a library card, but the numbers in the library card itself generally convey no meaning about the individual.) There are many different types of associated information, such as government identification information (e.g., Social Security numbers, driver's license numbers, security clearances, etc.), contact information (e.g., name, home addresses, phone numbers, email addresses, etc.), device identifiers (e.g., IP addresses, MAC address, browser cookies, etc.), property information (e.g., land titles, vehicle registration numbers, etc.), online authentication information (e.g., screen names, passwords, security tokens, etc.), and financial information (e.g., bank account numbers, credit card numbers, insurance details, etc.). Information in this category, since it does not describe an individual, has no inherent privacy implications itself. However, this information can be used to perpetrate actions that have privacy implications. For example, the PIN number of a bank card has no inherent privacy implications, but a third party might use a stolen PIN number to check someone's balance at a bank, an action which clearly has privacy implications.

Table 1: Types of information with examples for each.

Type of Information	Examples
Observable Information	Photographs, Videos, Emails, Recordings, etc.
Observed Information	Geolocation, Date of Birth, Search History, etc.
Computed Information	Advertising Profiles, Biometrics, Credit Scores, etc.
Associated Information	Social Security Numbers, IP Addresses, Land Titles, etc.

[9] Benjamin Wittes, "Database: Digital Privacy and the Mosaic," *Brookings Institution*, April 1, 2011, accessed October 26, 2017, https://www.brookings.edu/research/databuse-digital-privacy-and-the-mosaic/.

CATEGORIES OF INFORMATIONAL INJURY

Informational injuries are harms that result from the collection or misuse of information. There are generally three types of informational injuries: autonomy violations, discrimination, and economic harm.

Table 2: Types of informational injuries.

Type of Informational Injuries	Examples
Autonomy violations	Breaking attorney-client privilege; Hidden camera in bathroom
Discrimination	Denying loan based on race; Rejecting job applicant based on disability
Economic harm	Financial fraud based on identity theft

First, autonomy violations result in harm for consumers when information they consider sensitive and would prefer to keep private becomes public through involuntary means. Harms that arise from autonomy violations are often reputational or interpersonal. For example, the recording of a church confessional or a private conversation between a lawyer and a client can harm an individual's standing in his or her community by revealing information he or she may want kept secret. Similarly, an individual may have a significant interest in maintaining the privacy of an image of his or her body, and the mere release of the photograph can cause an injury. There are several tort laws in place that deal with these sorts of harms in civil cases: intrusion upon seclusion, public disclosure of private facts, and publicity which places a person in a false light in the public eye.[10] Some state laws also cover autonomy violations, such as voyeurism or "peeping tom" laws.[11]

Not all autonomy violations should necessarily be prohibited by law. Different people will have different opinions on what information should be public. In addition, some people may perceive an autonomy violation because they do not recall when they made the decision to allow a third party to collect and use their information (i.e. either by choosing to give consent or choosing to not opt-out). Indeed, some consumers are rationally ignorant of how third-parties use their information as they prefer not to read privacy notices.[12]

---

[10] William Prosser, "Privacy," California Law Review 48, (1960), 3, accessed October 24, 2017, http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3157&context=californialawreview

[11] "NDAA Voyeurism Compilation," National District Attorneys Association, 2010, accessed October 24, 2017, http://www.ndaa.org/pdf/Voyeurism%202010.pdf.

[12] Carlos Jensen, Colin Potts, and Christian Jensen, "Privacy Practices of internet Users: Self-Reports Versus Observed Behavior," Int. J. Human-Computer Studies 63 (2005) 203–227, accessed October 24, 2017, https://gnunet.org/sites/default/files/PrivacyPractices2005Jensen.pdf.

When this situation occurs, such as when Internet users see targeted advertisements for goods or services they had previously shopped for online, they may feel unease (i.e., consider this "creepy"). However, this type of scenario should not be considered an informational injury. These types of misperceptions about harms are likely to diminish with increased digital literacy.

Second, discrimination occurs when personal information is used to deny a person access to something, such as employment, housing, loans, or basic goods and services. There are many types of discrimination, including on the basis of age, class, disability, employment, language, gender, genetic information, national origin, pregnancy, race or ethnicity, religion, sex, sexual orientation, and more. For example, discrimination would occur if a bank used demographic information (e.g., age and sex) to deny a bank loan. The United States has several laws dedicated to criminalizing discrimination, including the Civil Rights Act of 1964, the Age Discrimination in Employment Act, the Americans with Disabilities Act, the Fair Credit Reporting Act, state anti-discrimination laws, and more, although many of these protections for workers do not apply to small business employers.[13]

Finally, economic harm results when a consumer suffers a financial loss or damage as a result of the misuse of PII. Most economy injuries that results from PII are identity theft, fraud, or larceny. Identity theft occurs when someone uses an individual's identity to access resources, such as credit cards, bank accounts, or other benefits.[14] For example, criminals can use personal information, such as Social Security numbers (SSNs), to open credit card accounts in their victim's name. Fraud occurs when a criminal uses deception to gain something of value from a victim, such as using a stolen credit card number to make purchases without the owner's consent. Many types of online attacks are designed to steal individuals' personal information to commit fraud and identity theft. In addition, criminals commit larceny by using stolen information, such as a password to a banking website, to directly steal personal property from their victim. These activities are illegal in the United States.

---

[13] "Laws Enforced by EEOC," *U.S. Equal Employment Opportunity Commission*, accessed October 24, 2017, https://www.eeoc.gov/laws/statutes/; Jerome Hunt, "A State-By-State Examination of Nondiscrimination Laws and Policies," *Center for American Progress Action Fund*, June 2012, https://www.americanprogress.org/wp-content/uploads/issues/2012/06/pdf/state_nondiscrimination.pdf

[14] "Identity Crimes," *Center for Identity Management and Information Protection*, accessed October 24, 2017, http://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm.

Policy Implications for Informational Injuries

As discussed above, not all information is the same. Different types of informational injuries can be found in each type of information, but some types of injuries are more commonly associated with a particular type of information. For example, a photograph may be used to perpetrate economic fraud, but this type of injury is generally secondary to other types of informational injuries for this type of information. As shown in Table 3, different types of information pose different privacy and security threats for individuals and each can result in different types of informational injuries. Policymakers should consider different responses for each type of injury.

Table 3: Types of informational injury based on types of information.

Type of Information	Primary Informational Injury
Observable Information	Autonomy violations
Observed Information	Autonomy violations or discrimination
Computed Information	Discrimination
Associated Information	Economic harm

Observable information involves information that individuals may want to keep private, and the mere release of the information can cause an injury. For example, most individuals want to keep intimate photographs of their body private. Distributing intimate photographs of an individual without that person's consent violates their autonomy.[15] This violation may cause additional reputational or interpersonal harms. To protect observable information, policymakers have a variety of tools to prevent harm, depending on the severity of privacy injury that the use of the data represents. First, policymakers can pursue laws and regulations that limit the collection of observable information with significant potential for harm. Examples of these policies include limitation on government surveillance and "Peeping Tom" laws. Second, policymakers can create restrictions on the harmful use or distribution of observable data. For example, they can pursue laws that criminalize the nonconsensual distribution of intimate photographs, or "revenge porn."[16] These policies balance strong protections of people's autonomy while ensuring that laws are not overly burdensome, such as prohibiting photography in public spaces.

[15] Daniel Castro and Alan McQuinn, "Why and How Congress Should Outlaw Revenge Porn," *Information technology and Innovation Foundation*, July 15, 2015, accessed October 24, 2017, https://itif.org/publications/2015/07/15/why-and-how-congress-should-outlaw-revenge-porn.
[16] Ibid.

Observed information can result in both autonomy violations and discrimination when revealed. First, there are many types of information in this category—such as medical records, video rental records, web browser history, and online purchases—where individuals have an expectation that they will be able to decide whether to make this information public. To mitigate informational injury in this category, policymakers have created certain targeted laws to constrain the sharing and use of certain observed information. For example, the Video Privacy Protection Act (VPPA) prevents unauthorized disclosure of personally-identifiable video rental and sale records.[17]

Second, there is some information in this category—such as age or disability—where, sometimes, but not always, individuals may be less concerned about their ability to keep the information private, and more concerned about others discriminating against them based on knowledge of this information. To mitigate this type of informational injury, policymakers have created laws to protect certain classes in areas like employment and housing discrimination.

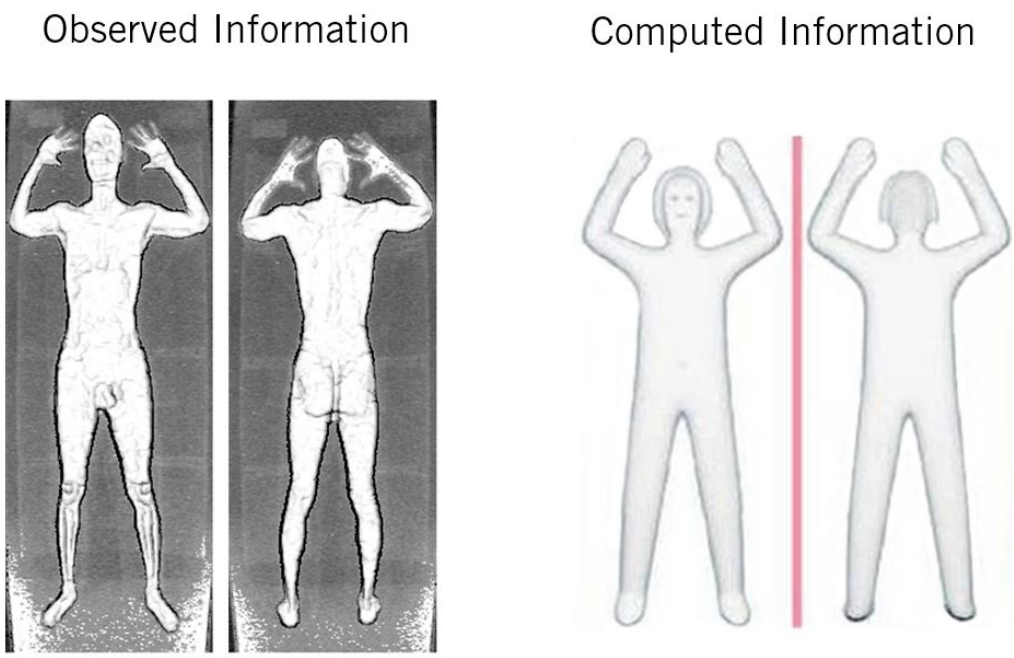
Individuals will make different decisions about what observable and observed information they want to make public. Some individuals may want to keep information about their sexual orientation private if that knowledge could disrupt their reputation, while others may value the public awareness of this trait within their community. However, policymakers should not create laws granting people autonomy to make decisions about all observable and observed information merely because a small group of people have privacy concerns. A small fraction of people, who privacy-researcher Alan Westin called "privacy fundamentalists," place such a high premium on their privacy that they are almost always unwilling to share their information under any condition.[18] These individuals are likely to perceive an injury from the release, or even the use, of most personal information, whether the data has a high intrinsic value or not. Policymakers should pursue laws and regulations that uphold general expectations of privacy and mitigate against demonstrated privacy harms in the use of observable and observed information. But they should also be cognizant of the fact that cultural norms and standards over what to make public may change over time, and create regulatory flexibility to allow the market to adjust to changing expectations. Striking this balance upholds privacy values while also protecting competing interests.

---

[17] 18 U.S. Code § 2710.

[18] Ponnurangam Kumaraguru and Lorrie Cranor, "Privacy Indexes: a survey of Westin's Studies," *Carnegie Mellon University*, December 2005, accessed October 24, 2017, http://repository.cmu.edu/cgi/viewcontent.cgi?article=1857&context=isr

Figure 1: Observed information versus computed information based on TSA scans.[19]



Computed information presents fewer privacy concerns for individuals than previous categories. For example, the TSA uses scanned images of an individual's body to generate generic outlines of that individual for TSA agents to view (Figure 1). These outlines do not, by themselves, identify the person but can be used to improve safety. However, this information can still result in discrimination if misused. A third party creates and controls this computed information to offer services to individuals. In many cases, the potential harm from computed information is discrimination or embarrassment, which results from third party discovery of this information. For example, Target compiled sales data with demographic data that it bought online to predict attributes about its customers and send them targeted coupons, such as for discounts for an expectant

[19] "Backscatter Large.jpg," *Wikimedia Commons*, accessed October 27, 2017, https://commons.wikimedia.org/wiki/File:Backscatter_large.jpg; and "Body image scanner avatar," *Wikimedia Commons*, accessed October 27, 2017, https://commons.wikimedia.org/wiki/File:Body_image_scanner_avatar.JPG.

mother.[20] However, this information, even if not accurate, could present potential injury to an individual if, for example, it was sold to a job candidate screening firm and an employer used this knowledge as a pretext to deny that person employment.

Because the primary harm in this category results from discrimination, problems often arises due to inadequate or outdated laws. For example, laws can forbid employers from discriminating based on sexual orientation when making hiring decisions, levy fines for abuse, and allow the potential employee to sue for damages. Social norms play a pivotal role in mitigating harm based on data in this category. For example, school teachers in the past would lose their jobs if they were married, making information on marital status highly sensitive.[21] The line for which classes of individuals should be protected can shift over time. For example, since 1973, 20 states and the District of Columbia have adopted laws to forbid employment discrimination based on sexual orientation and gender identity.[22]

In addition, sometimes the problem is that the information may be incorrect. In some cases, the solution to that problem is to allow individuals to correct the underlying information, such as how consumers can correct information that generates an incorrect credit score. Creating mechanisms that allow users to correct computed information can ensure it is accurate and up-to-date, and prevent some underlying issues.

Associated information is information that has no value on its own, but can be used in a way to create value (or cause harm). For example, while SSNs do not have any inherent value, government agencies, banks, hospitals, and others routinely use them, sometimes in combination with other personal information, to verify someone's identity, such as a bank before opening a new credit card account or a health insurer before paying out a medical claim. There are many types of associated information, often assigned by a third party, such as unique device identifiers, passwords, PIN numbers, passport numbers, and drivers' license numbers. Harms

---

[20] Charles Duhigg, "How Companies Learn Your Secrets," *New York Times*, February 12, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

[21] Valerie Strauss, Local, "Rules for teachers in 1872: No marriage for women or barber shops for men," *Washington Post*, June 2, 2011, accessed October 24, 2017, https://www.washingtonpost.com/blogs/answer-sheet/post/rules-for-teachers-in-1872-no-marriage-for-women-or-barber-shops-for-men/2011/06/01/AGTSSpGH_blog.html?utm_term=.fd506f3130c3

[22] "Non-Discrimination Laws," *Movement Advancement Project*, accessed October 24, 2017, http://www.lgbtmap.org/equality-maps/non_discrimination_laws; Linda Mooney, David Knox, Caroline Schnacht, *Understanding Social Problems* (Wadsworth: Cengage Learning, 2007), 464-467, *Google Books*, accessed October 24, 2017, https://books.google.com/books?id=1Zb3-2UxHyUC&pg=PT493&lpg=PT493#v=onepage&q&f=false

from the misuse of this information are usually economic in nature, resulting from larceny, malware, spam, fraud, or identity theft.

Policymakers can mitigate against the abuse and misuse of associated information by promoting laws and regulations that increase security, especially through better technologies and policies for electronic identification and authentication in both commercial and government applications.[23] Policymakers should replace outdated systems, such as SSNs, with a secure alternatives that effectively turns other forms of personal information into worthless trivia.[24] Policymakers should generally allow organizations to collect and share this information provided they disclose to individuals their practices.

Levels of PII Collection and Use

The way in which a third party collects and uses PII affects the potential for harm. As shown in Table 3, there are generally four levels of PII collection and use, each with a different level of risk for informational injury.

Table 3: Levels of collection and use of PII.

Levels	Description	Potential for Informational Injury
Level 0	No collection and use	None
Level 1	Collection and no use.	Low
Level 2	Collection and use (no human)	Low
Level 3	Collection and use (with human)	High

In level 0, a third party does not collect or use PII. The third party may use anonymized data that is not linked or reasonably linkable to an individual. For example, a company may gather geospatial data from satellites to generate maps. Because no PII is collected, there is virtually no risk for informational injury.

In level 1, companies collect PII but do not use it. The third party may have data lying dormant on a server. For example, some companies inadvertently collect information as a result of a coding error, but no human sees this information and the company does not use it.[25] In most cases, there is little risk of informational

[23] Daniel Castro, "Electronic Identification," *Information technology and Innovation Foundation,* September 2011, accessed October 24, 2017, http://www.itif.org/files/2011-e-id-report-final.pdf
[24] Daniel Castro, "Time to Retire Social Security Numbers," *Real Clear Policy*, September 16, 2017, accessed October 24, 2017, http://www.realclearpolicy.com/articles/2017/09/16/time_to_retire_social_security_numbers_110358.html.
[25] For an example of accidental collection, please see: Alan Eustace, "WiFi data collection: An update," *Google*, May 14, 2010, accessed October 26, 2017, https://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html.

injury to individuals when a third party collects, but does not use, PII. The exception is for certain types of sensitive observable information, such as intimate photos taken where someone has an expectation of privacy, where the mere collection of the information may violate their autonomy.

In level 2, a third party collects and uses PII, but no human sees the data. Instead, all data handling occurs with computers. For example, email providers may scan their customers messages to detect spam, malware, or offer other features. Similarly, Google used to scan email messages to generate targeted advertisements.[26] In these cases, no human accesses the personal information so the risk of informational injury remains low.

In level 3, a third party collects and uses PII and humans see the data. For example, the staff working in the human resources department may review PII of other employees, such as payroll information or tax forms. Similarly, various hospital workers may review personal medical information in patient records as part of their routine duties. Many, if not most, of users' privacy concerns are about ensuring that other people do not see something they consider sensitive information. For example, most Internet users do not have any real objection to their Internet service provider having temporary digital records of which sites they visit, but they do not want this information to be made available to another person without their permission.

Increased use of computers to process personal data can lead to increases in user privacy. In fact, a 2017 survey shows that individuals prefer dealing with remote entities that use computers to process data, rather than "immediately-present people that could judge them."[27] For example, consumers generally prefer to purchase sensitive items (e.g., condoms) online or through a self-checkout than from a human sales clerk.[28] Policymakers who want to decrease the risk of informational injury should support efforts to make more processes digital to avoid level 3.

---

[26] Google announced in June 2017 that it would no longer scan email contents to generate personalized ads, but would get this data from other sources of observed data. Diana Greene, "As G Suite gains traction in the enterprise, G Suite's Gmail and consumer Gmail to more closely align," *Google*, June 23, 2017, accessed October 24, 2017, https://blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/.

[27] Benjamin Wittes and Emma Kohse, "The Privacy Paradox II: Measuring the Privacy Benefits of Privacy Threats," *Brookings Institution*, January 2017, accessed October 24, 2017, https://www.brookings.edu/wp-content/uploads/2017/01/privacy-paper.pdf.

[28] Ibid.

CONCLUSION

When evaluating how consumers can be harmed through the misuse of their information, the FTC should use a more detailed typology for information and the harms that result from that information. In addition, as discussed above, limiting data collection and data sharing is an inappropriate method to reduce informational injury in many situations. Consumers are better served by more targeted rules that address specific harms. Only by narrowly tailoring these definitions and pursuing informational injury cases based on demonstrated harm can the FTC both protect consumer privacy and advance innovation.

Sincerely,

Daniel Castro
Vice President, Information Technology and Innovation Foundation

Alan McQuinn
Research Analyst, Information Technology and Innovation Foundation