accenture

Strategy | Consulting | Digital | Technology | Operations

Accenture Labs

Informed consent and data in motion

Preventing unintended consequences through stronger data ethics

High performance. Delivered.

As the capabilities of data analytics push further ahead, the risks grow for those whose data is collected. The likelihood that previously anonymized data may become de-anonymized increases with each new advance. Inherent biases are introduced through algorithm selection, training data, and hypothesis testing, which can result in automated decision-making that is biased.

Analytics can uncover information previously unavailable: it's already possible, in some cases, for governments to use big data analytics to discover crimes that otherwise would have remained secret. What should be done with that information? Is that an easier question to answer when the culprits are terrorists or sex offenders? What if the government in question is an oppressive regime and the crime is breaking a law related to censorship? It is difficult to imagine the potential harm of unintended consequences in these areas, let alone take active steps to prepare for that harm, mitigate it, and recover from it.

One prudent approach to minimize the potential for harm is to gain informed consent from individuals who are disclosing data. With the increasing presence of (and reliance on) digital technologies, it is critical for individuals to understand what they are consenting to by sharing data. Similarly, it's important to help designers and developers minimize unintended harm from the use of that data. In the field of data science, practitioners must integrate ethical decision-making into most discussions about data to avoid unforeseen risks that arise from the complex movement of data through a wide diversity of systems. Ethical behavior in this context is about the treatment, protection and transformation of data moving between systems ("data in motion")—not just recorded, static data ("data at rest"). This paper explores how the concept of informed consent in a world of "data in motion" might be addressed to help apply the doctrine of doing no harm in the digital age.

Complexities of data in motion

In order to truly consider informed consent, it is important to understand the concepts of "data at rest" and "data in motion," particularly in the context of contemporary digital systems.

Traditionally, data gathered for electronic recordkeeping was in the same paradigm as files in a filing cabinet. Data was recorded by a human at some point, filed away, and retrieved (and perhaps updated) as needed. Data that was no longer relevant would be discarded to make room for new data.

Early digital systems were similar: data was input by human beings, created by computer systems, or sensed within an environment, and then more or less filed away to be retrieved later, when needed.

Modern data management can be mapped to three key stages:

1. Disclosing / Sensing—humans or machines that gather and record data.

2. Manipulating / Processing— aggregation, transformation, and/or analysis that turns data into useful information.

3. Consuming / Applying—a person or machine uses information to derive insights that can then be used to affect change.

Historically, digital systems were not as interoperable and networked as they are now, and so data could be thought of as being "at rest"—stored statically, just like the files in filing cabinets of the past. But today, some

Figure 1: Guidelines for avoiding harm

	DATA AT REST	DATA IN MOTION
Data Disclosure	Data may be sourced from archives or other backups **Guideline:** Ensure the context of original consent is known and respected; data security practices should be revisited on a regular basis to minimize risk of accidental disclosure. Aggregation of data from multiple sources often represents a new context for disclosure; have the responsible parties made a meaningful effort to renew informed consent agreements for this new context?	Data is collected in real-time from machine sensors, automated processes, or human input; while in motion, data may or may not be retained, reshaped, corrupted, disclosed, etc. **Guideline:** Be respectful of data disclosers and the individuals behind the data. Protect the integrity and security of data throughout networks and supply chains. Only collect the minimum amount of data needed for a specific application. Avoid collecting personally identifiable information, or any associated meta-data whenever possible. Maximize preservation of provenance.
Data Manipulation	Data is stored locally without widespread distribution channels; all transformations happen locally **Guideline:** Set up a secure environment for handling static data so the risk of security breaches is minimized and data is not mistakenly shared with external networks. Data movement and transformation should be fully auditable.	Data is actively being moved or aggregated; data transformations use multiple datasets or API calls which might be from multiple parties; the Internet may be used **Guideline:** Ensure that data moving between networks and cloud service providers is encrypted; shared datasets should strive to minimize the amount of data shared and anonymize as much as possible. Be sure to destroy any temporary databases that contain aggregated data. Are research outcomes consistent with the discloser's original intentions?
Data Consumption	Data analytics processes do not rely on live or real-time updates **Guideline:** Consider how comfortable data disclosers would be with how the derived insights are being applied. Gain consent, preferably informed consent, from data disclosers for application-specific uses of data.	Data insights could be context-aware, informed by sensors, or might benefit from streamed data or API calls **Guideline:** The data at rest guidelines for data consumption are equally important here. In addition, adhere to any license agreements associated with the APIs being used. Encrypt data. Be conscious of the lack of control over streamed data once it is broadcast. Streaming data also has a unique range of potential harms—the ability to track individuals, deciphering network vulnerabilities, etc.

data is in near-constant motion. When we access social media sites, we're not just pulling static data from some digital filing cabinet—we are accessing data which is in constant transformation. For example, algorithms shift which news stories are displayed to us based on an ever-evolving model around our tastes and the tastes of other users. An action taken in an app, like an online retailer, connected to a user's social media account could change the content delivered to a user. Managing the complexity of consent and potential harms in this environment is much harder than the connection between traditional market research and mass-purchase, broadcast advertising.

This data in motion is much harder to comprehend at scale. The chaotic effects of multiple, interoperable systems and their data playing off each other makes it difficult for design and development stakeholders to see the big picture of how data might affect their users—much less communicate to those users for the purposes of informed consent or doing no harm.

Data in motion can be relatively straightforward in the context of the flow of interactions through each stage of disclosing, manipulating, and consuming data. However, although it can be tempting to think of data as a file moving from one filing cabinet to another, it is, in fact, something more dynamic, which is being manipulated in many different ways in many different locations, more or less simultaneously. It becomes even more ambiguous when a lack of interaction with a piece of data could still be used to draw conclusions about a user that they might otherwise keep private.

For example, ride-sharing apps need to collect location information about drivers and passengers to ensure the service is being delivered. This makes sense in "the moment" of using the app. However, if the app's consent agreement allows location data to be collected regardless of whether or not the driver or rider is actually using the app, a user may be passively providing their location information without being actively aware of that fact. In such cases, the application may be inferring things about that passenger's interest in various goods or services based on the locations they travel to, even when they're not using the app.

Given that location data may be moving through mapping APIs, or used by the app provider in numerous ways, a user has little insight into the real-time use of their data and the different parties with whom that data may be shared. For users of the ride-sharing app, this may cause concern that their location data is being used to profile their time spent outside the app—information that could be significant if, for example, an algorithm determines that a driver who has installed the app is also driving with a competing ride-sharing provider.[1] Without clear consent agreements, interpretation of where data moves and how it is used becomes challenging for the user and can erode the trust that their best interests are being served.

"This data in motion is much harder to comprehend at scale. The chaotic effects of multiple, interoperable systems and their data playing off each other makes it difficult for design and development stakeholders to see the big picture of how data might affect their users."

Understanding data diplomacy

Trading data among multiple organizations can make data more useful and information more insightful. As a discipline, this practice requires the ability to predict potential effects when data is combined or used in new ways or new combinations, and is best aided when data's movement can be recorded in a way that makes tracking provenance possible when failures occur. But just as diplomats must consider many complex and sometimes unpredictable risks and opportunities when engaging across borders, so too must leaders and developers.

Organizations must be willing to devote at least as much time to considering the effects of this data-sharing as they are willing to look at its monetization options. They must also find a common language with other organizations—and end-users—to determine what is an effective and acceptable use of data. Informed consent requires that data diplomats—be they business executives, application developers, or marketing teams, among many others—communicate proactively about the potential pitfalls of data exposure.[2]

Organizations which are effective at communicating their data-sharing efforts stand to win the trust of users. These users will be willing to take a (measured) risk in sharing their data with the promise of a return of more useful data and information, less expensive services, or other benefits.

Designing a system for informed consent

Systems and applications should be designed with adoption in mind. Given the chaotic nature of data in motion, designers need to understand that users may not fully consider (or be aware of) the entirety of their data's use. With this in mind, it is important that data-driven products are designed to capture user expectations.

Understanding the user's needs and desires

"Persona modeling" for human actors

To ensure that the privacy and harm risks for all parties in a data supply-chain are properly addressed and managed, it's essential to create maps of the various emotional, social, and functional tasks humans want or need to do. Developing "persona models", which are mapped to real-life interviews after product or application releases, is a critical component of agile development. Such models are also valuable to agile approaches for discovering harms previously unknown to developers.

For example, transgender and domestic violence use-cases were not fully considered in Facebook's push for users to go by real names (or "authentic names" in Facebook's terminology). Because Facebook did not fully conceive of the many ways people use names—or why they might not share their legal names—users were required to title their profiles with their legal names. This presented a difficult situation to these disadvantaged users, and prompted a group of individuals to write to Facebook expressing their concern.[3] Facebook has since introduced a more nuanced interpretation of its naming policy, providing a doctrinal guide for both users and Facebook staff which indicates the "why" of authentic names while still precluding false names used for impersonation.[4] It outlines a much broader set of options for identity verification and appeals, and demonstrates some line of sight between Facebook's users, front-line employees, developers, and leadership.

In *Positive Computing: Technology for Wellbeing and Human Potential*, the authors explain that research into "proving" a positive or negative outcome of any one technology is nearly impossible because of the complexity of modern systems.[5] Instead, the authors (and many multidisciplinary technologists) guide designers of such systems to focus on intentions and outcomes.

The *why* of a user's use of a given technology is as important as the *how* of their use. If a user is clear about why they are using a system, and the designers of that system also have some idea of why the user is sharing data within that system, proactive, *positive* choices about the universe of data transformations to engage in—and those to avoid—can be baked in. For example, a professional social network with multiple subscription options or profile types for its users, such as for job-seekers vs sales professionals, could infer (and verify) that users who are job-seekers might react *negatively* to disclosure of new activity on their profiles. This could alert their current employer that they are exploring other jobs—potentially causing unnecessary stress or even premature loss of employment. Conversely, sales-focused users might react *positively* to the disclosure of the activity on their profiles. Proactively (and explicitly) asking the "why" of a user's disclosure of data about them, and verifying the "why" when new activity happens, can drastically lessen the likelihood that user intent will be misunderstood.

Persona modeling for machine (or "thing") actors

The Internet of Things can in some ways be better thought of as a Social Network of Things—networks of devices and data with their own relationships and decisions to make. By modeling the various "needs" of a device to connect with other devices to pass data, and use that data to make decisions, it is easier to identify data paths that are potentially vulnerable to unauthorized sharing, or to which parties might gain access without approval.

Getting informed consent: communicating possibilities

Informed consent, as it relates to data collection and use, requires, at the least, two elements to be met.

In order for consent to be informed, end-users must understand what data is being gathered, who will have access to it, and how it will be used. However, ethically, it is also incumbent upon organizations gathering data to ensure that potential harms are conceived of and shared with users. These harms should be shared in a way users can understand, and proportionate to their potential impact and the statistical likelihood of their occurrence. It's possible that companies managing private data could be incentivized or required to advertise the "side effects" of sharing data the same way drug companies must do in their advertisements.

In order to request and achieve informed consent, organizations must first understand, and then clearly communicate, how they and their partners will 1) use data and 2) ensure that the data will not be accessed or used in ways that fall outside of the scope that has been, or will be, communicated to end-users. This is the "consent" element.

Common sense dictates that users should also derive value from the disclosure of the data they share in some way. If not, no matter how good the messaging around the data usage is, companies will struggle to receive consent.

The requirements necessary for informed consent fall under the larger concept of "data literacy"—awareness of how digital data is affecting all parts of modern life. Discussion of data literacy raises questions about the feasibility and responsibility for education around data collection and use on a public and enterprise level. How much time and attention should people reasonably be expected to devote to understanding the intricacies and implications of data collection and use? What is the level of responsibility that should be placed on organizations that play a role in how users interact with consent?

Selecting "accept" on an End-User License Agreement (EULA) may count as informed consent from a legal perspective. But is the information in the small print really accessible to most users in a way that satisfies the ethical challenges surrounding data monetization, data sharing, and the myriad other ways that individual data may be used, or could be used in the future? The uses of data and the distinctions of who benefits from those uses (and how) are constantly evolving and in flux, and imagining those uses is part of data literacy. As a result, it's difficult to define an endpoint for consent in this context. There is perhaps no such thing as being truly data-literate in the general sense; we can only attend to specific uses and types of data, and on an organizational level, commit to transparency and iteration of consent agreements as organizations continue to explore the value and dangers of personal data as a resource in the digital age. End-user license agreements are premised on the idea that organizations and end-users are digitally literate—prepared to imagine the impact of their disclosures—and that both organizations and end-users speak the same language about data. Without that awareness, and that shared language, informed consent in EULAs is not present.

With the information and understanding required for consent and ethical use of data constantly changing and hard to measure, best practices for organizations that collect and use data must focus on improving transparency and communicating intent. From a customer and partner relationship perspective, there's an obvious benefit for organizations which make a visible and genuine effort to provide information about their data use. Critically, that information must be provided in terms that everyday users can understand and accept—or reject—with confidence. One might also propose that the process of converting the most common jargon in EULAs and Terms of Service (TOS) documents to everyday language would go a long way toward having people within organizations understand, and be honest with themselves, about the ethical nuances of data collection and use.

> "If you want to build loyalty, spend less time using data to tell customers about you, and spend more time telling them something about themselves."
>
> —Mark Bonchek, PhD, Harvard Business Review[6]

There is a disincentive for many companies to disclose data uses when their data use is either not in the obvious interest of the user (e.g. marketing/advertising emails) or because incomplete understanding of how data is actually collected, transformed and protected—or made vulnerable—scares users. An example of this gray area created by a lack of digital literacy can be seen in misunderstandings between Google and some of its users about how it was (or was not) using the content of customer emails to provide targeted ads through free versions of its gmail service.[7] Because users did not understand (and Google did not effectively communicate) where customer data was being processed and what the implications of that were for users, stories of upset customers raised skepticism about the integrity of Google's handling of private information.

Ethical practice is particularly complex when intent, consent, and benefit are subject to very different interpretation. Consider Facebook's massive, longitudinal study on the impact a positively or negatively skewed news-feed had on a user's own posts.[8] When this study was announced (after the fact), there was immediate backlash. While Facebook may have been within the bounds of their EULA to conduct this study, the response shows that they had misjudged how users would react. Users responded poorly to the news that their behavior was being studied based on a manipulation of the information being presented in their feeds. In addition, it was unclear whether their unwitting participation in the study would lead to better products and services (which might at least provide some positive outcome), or if their results would be used to steer spending or ad placement (which might make the study feel exploitative). This study existed in a controlled environment with an institutional review board (IRB), responsible for ensuring study participants were treated fairly, but the response when the information was made public was not entirely positive.[9] In response to this reaction, Facebook has taken steps to publish a framework that details the guidelines and best practices they will utilize in research, with the goal of preventing miscommunication around future studies.[10, 11] However, typical A/B (and multiple variable) software testing is not required to go through these same review processes. When changing variables 'A' and 'B' in ways that could have real impacts on emotional response (or in the physical world), organizations need to be clear about how they intend to use the resulting data.

Data transformation and use

Informed consent requires sufficient understanding by all parties of how data will be *transformed* into meaningful information. It is in this transformation that many of the unintended consequences of data sharing and data collaboration take form. Use implies access, but the real issue at hand is accessing data to transform it into something else—information. This information is then used on its own, as insight, or to trigger actions. Whether those actions are executed by humans after manual digestion of those insights, or those actions are a response to logic programmed in advance by humans, the world of human ethics collides with the world of binary logic in a messy, hard-to-track decision tree with effects often more evocative of chaos theory than simple branched charts. Given this complexity, the best approach to managing user expectations around data transformation and use of resulting information is to provide clarity at the time of data collection as to intended and potential future uses. The goal is to ensure that meaningful consent is achieved.

Complexities of law and jurisdiction

While it is a common method of securing consent from a legal perspective, requiring users to grant use of data before accessing necessary services is often not in the user's best interests. Moreover, such agreements may play on a lack of data fluency, even more so with use of complex legal language. End-User License Agreements (EULAs) and Terms of Service (TOS) agreements are the places where most of these data exchange agreements occur. The Electronic Frontier Foundation has been warning users of the rights they relinquish in these agreements since at least 2005. Case law in the United States and other jurisdictions provides limited protections to end-users and corporations, so the enforceability of EULAs and TOS agreements varies by jurisdiction.

There has been widespread debate over enforceability within complex data relationships—especially those in which companies, users, and strategic data partners may exist in jurisdictions with conflicting case law. Perhaps most notable is the European Union's decision to insist that all European user data be stored on servers housed in the EU, both to protect users from environments with less privacy-focused regulatory controls than the EU, and also to prevent government-sponsored surveillance and tampering.[12] However, this approach is incomplete because it is based on the belief that data being used is primarily at rest—stored statically—and primarily accessed by the same parties who stored it, on behalf of the same users. When data is often in motion between various servers and algorithms with massively complex interdependencies across state and corporate lines, such regulation provides little real protection for users. At the other end of the spectrum, strict interpretation could silo data about users in a way that limits meaningful use of the data by the people furnishing, storing or transforming it.

Mechanisms for consent

Informed consent is especially challenging in the digital age. The rapid transit of data from server to server, transformed through algorithms and intermingling with other data, means that the intentions and realities of each organization and individual that touches that data must to be understood in order to give fully informed consent. This happens in one of two ways: either through data-fluent, savvy users with access to transparency throughout the data supply chain; or through proxies of trust, where a trusted third party, approach, or standard is used as a proxy for trust in all entities along the data supply chain. For the latter category, there are multiple approaches to establishing trusted data use:

Trusted party

Facebook, Google, other single-sign-on and API aggregators, consortia or other trusted groups assure users that private data is passing through only systems with certain standards of protection.

Vetting approach

Apple's App Store (and how, for example, its review process caught data leaks introduced across many apps through spurious analytics tools for developers) is an example of an approach where users trust new services (provided by apps, in this case) based on their vetting by a familiar party.

Kit (trusted core) approach

Software Development Kits (SDKs) are sets of common tools, often hosted by a single party or consortium, which empower app developers to create value without having to invent their own frameworks and tools. Apple's HealthKit and related ResearchKit manage data about users, and if a user trusts HealthKit's standard for privacy, they may be more likely to use apps which abide by the privacy standards set out by such an ecosystem.

Industry standards and compliance

Trust can be established through industry standards and/or governmental compliance, like health codes, security clearances or other commit-and-audit-by-third-party strategies. These allow organizations to opt-in to standards that are sufficient to meet government regulations.

Embedded trust/trusted technologies

Technology-based strategies (such as blockchain) assure users that their data is protected not on the basis of where it is stored, but by the mechanisms that encrypt data, record, and provide proof that exchanges have occurred. In-hardware protection, such as specific forms of encryption or embedded SIM cards, can also be considered a point of embedded trust.

Communicating and verifying intent

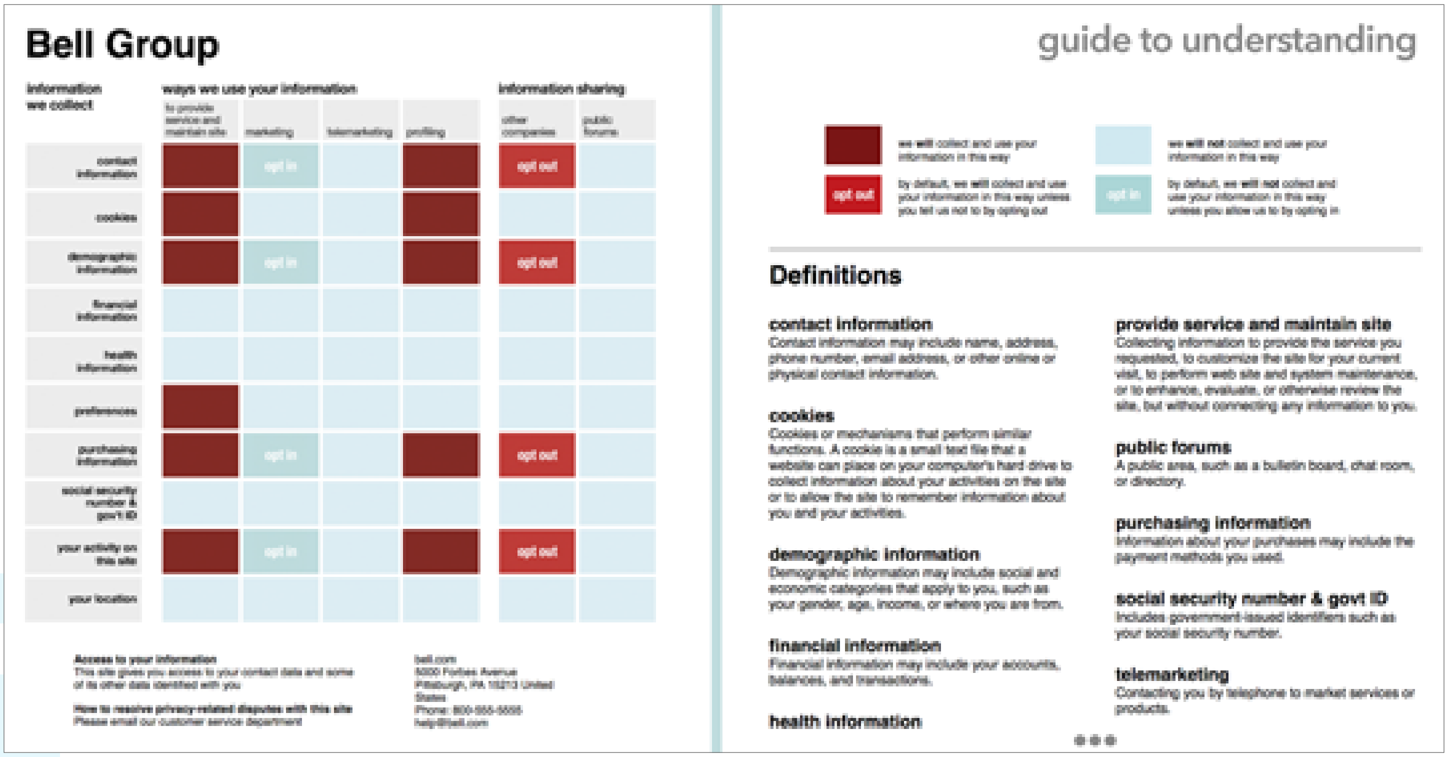
Users must be aware of the intended uses of the data they furnish to an app or service in order to provide informed consent. This communication is not complete if users don't actually know or understand what data already exists or could be gathered by devices, such as location data in a mobile device or a microphone embedded in a smart television remote which they didn't realize is "voice-capable."

Once users understand both what the data being gathered about them might consist of and also how an application or service intends to use that data, *informed* consent can be established. However, it's critical to ensure that the communication generated to achieve consent is created using language that truly informs, rather than obfuscates.

From obfuscation to clarity: Decoding the EULA

While End-User License Agreements may use technical language that renders them insufficient to achieve truly informed consent (as discussed earlier), there are several existing models for translating the complex technical concepts of user consent agreements into accessible language for the public. One such model is the "Privacy Nutrition Label" developed by a joint team from Carnegie Mellon University and Microsoft.[13] Their project catalogued the types of information required on safety and nutritional labels and approached the problem of informed consent and data fluency as a design problem. The result of their work is a comparison chart which distinguishes opt-in data from that which is automatically collected, states how various types of data would be used, and includes a glossary of terms for further clarification (Figure 2).[14]

Figure 2



Bell Group

information we collect	ways we use your information				information sharing	
	to provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information	■	opt in	□	■	opt out	□
cookies	■	□	□	■	□	□
demographic information	■	opt in	□	■	opt out	□
financial information	□	□	□	□	□	□
health information	□	□	□	□	□	□
preferences	■	□	□	□	□	□
purchasing information	■	opt in	□	■	opt out	□
social security number & gov't ID	□	□	□	□	□	□
your activity on this site	■	opt in	□	■	opt out	□
your location	□	□	□	□	□	□

Access to your information
This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site
Please email our customer service department

bell.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United
States
Phone: 800-555-5555
help@bell.com

guide to understanding

■ we will collect and use your information in this way

□ we will not collect and use your information in this way

opt out: by default, we will collect and use your information in this way unless you tell us not to by opting out

opt in: by default, we will not collect and use your information in this way unless you allow us to by opting in

Definitions

contact information
Contact information may include name, address, phone number, email address, or other online or physical contact information.

cookies
Cookies or mechanisms that perform similar functions. A cookie is a small text file that a website can place on your computer's hard drive to collect information about your activities on the site or to allow the site to remember information about you and your activities.

demographic information
Demographic information may include social and economic categories that apply to you, such as your gender, age, income, or where you are from.

financial information
Financial information may include your accounts, balances, and transactions.

health information

provide service and maintain site
Collecting information to provide the service you requested, to customize the site for your current visit, to perform web site and system maintenance, or to enhance, evaluate, or otherwise review the site, but without connecting any information to you.

public forums
A public area, such as a bulletin board, chat room, or directory.

purchasing information
Information about your purchases may include the payment methods you used.

social security number & govt ID
Includes government-issued identifiers such as your social security number.

telemarketing
Contacting you by telephone to market services or products.

• • •

Reprinted with permission from Patrick Gage Kelley.

The Carnegie Mellon's CyLab Usable Privacy and Security Laboratory has developed an online platform that allows users to decode complex privacy agreements for themselves.[15] Their website lets users search by URL or website name, then pulls the privacy agreement language from the source site. The agreement is then presented to the user in its original form, along with a sidebar that categorizes each statement by function or topic, and offers common language explanations clause-by-clause.[16] An added benefit of this platform is that the common language phrases are visually linked to the "legalese" in the original—the translated text is highlighted when mousing over the corresponding explanation. This allows users to gradually become familiar with the practical meaning of the more complex privacy notice language, encouraging and enabling them to read and translate data-use agreements in the future, without the need for a translation tool. In this way, this particular solution acts as a vehicle to further data fluency, while simultaneously preparing the user to self-educate in the future.

Both of these solutions point to an important consideration: not all users understand information through the same mediums. Some people need visual examples and graphical representations of information, others prefer concise statements that focus on consequences and impact, and others may want to know all the details. As we consider what informed consent requires in regard to communication, education, and understanding, adult learning styles become a design consideration in a way that legal departments and traditional UX developers cannot be left to solve for on their own.

Managing consent over time

The best implementations of informed consent manage consent not just at the beginning of using a service, but over time, especially at critical junctures.

Privacy checkups: adjusting and maintaining consent while educating users

One example of actively managed consent over time can be found in Apple's Location Services function within iOS. It prompts users not just when an app first asks to know the location of the user, but also when an app has been using the phone's location in the background for an extended period, to *confirm* whether the user intended to let that app continue accessing their location. This both ensures that the user consents initially to a specific app's request (rather than simply granting access to all apps), but also that they can continue to enjoy the benefits of allowing location access or revoke consent to that usage if they change their mind.

In another example of actively managed consent over time, Google's security check up helps Google users understand how the data they disclose is used in delivering Google products and services.[17] The six-step process, which is periodically offered to users but can also be accessed any time on request, walks the user through different permissions that may or may not have been granted when the user last agreed to Google's terms and conditions. Users are given the ability to modify these permissions either through restricting data use, pausing data collection, or updating basic information like telephone numbers. For example, if a user does not want to be served targeted ads, the checkup allows them to turn off targeting entirely or to adjust the topics for ads that Google deemed relevant to that user. As terms of services and end-user license agreements are updated, reviewing this information allows users to reconfirm that their expectations around data use are being met, and modify permissions if they are not.

Monitoring and managing

Outcome monitoring and discovering harm

With the advent of mainstream IoT devices, a sensor on a device may give a user feedback in the form of a raw number that reflects something about the state of their environment. If the user takes this information at face-value, they may start to think less about the device providing the feedback and focus instead on the number itself. This shift in attention is important because overlooking the device or system that provides feedback suggests that how data is handled and any algorithms used to process the data are also being overlooked. The failure to consider these underlying interactions can result in unintended risks.

Take the example of the use of algorithms to create risk assessment scores that rate a defendant's risk of committing future crime. Now widespread in the US justice system, these risk assessments were recently the subject of an in-depth investigation by ProPublica, an independent newsroom producing investigative journalism in the public interest.[18] In 2014, the US Attorney General raised concerns that these scores could be introducing bias to the courts (where they are used to inform decisions on bail, sentencing, and probation). This algorithmic process has been shown to be unreliable in forecasting certain kinds of crime. In fact, in an instance investigated by ProPublica, based on the risk scores assigned to over 7,000 people arrested in a single Florida county in 2013 and 2014, the algorithm used was little more reliable than tossing a coin in its ability to accurately identify re-offenders.

With analytics and machine learning, algorithms can be trained to notice where there has been customer upset, and bring it to the attention of a real human—in other words, detecting that harm may have been done and bringing it to the attention of developers and other stakeholders. On social media, sentiment analysis (a set of tools and practices which deconstruct written language and user behaviors to detect mood) could be used to identify situations where a piece of data shared about a user is causing emotional (and potentially physical) harm.

Take the example of a user of a social network uploading a picture of another user and "tagging" them in that picture. If that second user starts reacting negatively in comment threads or receiving negative messages from others, machine learning could identify these situations and escalate them to moderators, presenting an opportunity for that user to "untag" themselves or request removal of the photograph in question. Such an approach could go further by then alerting developers and other business teams to consider such scenarios in their user personas and user stories for subsequent app updates, consent and permissions management approaches. This secondary feedback is key in making sure lessons learned are acted upon and that the appropriate corrective action is taken.

"With analytics and machine learning, algorithms can be trained to notice where there has been customer upset, and bring it to the attention of a real human."

Monitoring data transformations through user interviews

Interviewing users who have experienced harm can uncover misunderstandings in the way users are perceiving or using applications. This is not placing the blame on users, but can rather be used to determine areas where better communication may be required. Noticing where users say that a use or disclosure of data was not appropriate is a form of qualitative forensics which can be linked to other, quantitative approaches like behavioral analytics. When users see an app or service that feels uncomfortable, that's an indication that consent may not be in place. But information about this discomfort rarely reaches developers or business stakeholders unless they cultivate—and systematize—curiosity about and empathy for users.

In order to think critically and spot potential harms to users, employees must have a working knowledge of how data moves and is transformed, how data (and users) are threatened by cyber-security breaches, and what end-users expected and consented their data could be used for. This goes for IT stakeholders, but also employees in general, given the increasingly digital nature of corporations across entire companies. Regularly updating the shared "world view" of the organization with both direct and analytics-sourced input from users is an important first step. Once it's been taken, it can be followed by creating feedback loops into the software development process from both human and machine sources. This will enable empathy for users to be systematized into actionable updates of practices and programming.

Forensic analysis

Forensic analysis of data breaches is becoming more commonplace when data holders experience cyberattacks; similar methods can be used to track data through various servers and applications to determine where personally identifying data might be vulnerable to disclosure, or has been processed in a way contrary to the intent of the user or designers. However, most organizations are not yet prepared to track data well enough to discover, much less mitigate, harms to users.

Continual discovery of potential harms

Google is faced with a conundrum: if its machine-learning discovers that a user may have a medical condition, based on what that user is searching for, is it ethical to tell the user? Or unethical? A recent article by Fast.co Design explored this concept:[19]

"If Google or another technology company has the ability to spot that I have cancer before I do, should it ethically have to tell me? As complicated as this question sounds, it turns out that most experts I asked—ranging from an ethicist to a doctor to a UX specialist—agreed on the solution. Google, along with Facebook, Apple, and their peers, should offer consumers the chance to opt-in to medical alerts."

Such conundrums are not limited to search results, but the uniquely personal (and potentially emotionally and physically harmful) impact of medical analytics is still a nascent conversation that neither healthcare providers nor technology companies are fully prepared to enter into—yet.

Leaders can learn from Google's example by creating ways for end-users, "observers" (in this case, medical professionals and other researchers), developers, and executives to discover potential harms—even after product launches.

"The reality is few organizations are currently able to show you the full impact of a breach—few are able to identify all of the systems that were breached, much less what specific data could have been compromised. Understanding the scope of the damage/harm is predicated on having both the right mindset and logging and monitoring in place."

—Lisa O'Connor, Managing Director, Security R&D, Accenture

Mitigating harm

Avoiding harm and continuing to seek and clarify informed consent is vitally important. But what happens when a harm is actually discovered? Mitigation of harms takes many forms, and can involve nearly every part of an organization—especially when harms are not immediately noticed or their scope is large.

Scope control and fail-safes

Data-related harms usually occur in one of two categories: unintended disclosure of raw data (such as photos of a user or their credit-card information) or improper decisions that have been made based on data about a user. These decisions can be made by humans (such as a decision on whether or not to prescribe a medication), hybrid decisions (such as a credit report-influenced decision whether to offer a loan) or machine decisions (such as automatic re-routing of vehicles based on traffic data). Strategies to mitigate such harm and respond to it when it occurs depend on the types of decisions being made.

Revocation and distributed deletion

While pre-release design is critical to meet the "do no harm" expectation, designing with the ability to adapt post-release is equally critical. For example, a social network in which users directly offer up data about themselves (whether for public or private consumption) would likely be launched with privacy controls available from day one. However, the system's owners may find that users are not aware of the available privacy controls, and introduce a feature whereby users are informed/reminded of the available settings. In such a case, users should be able to *retroactively* affect their past shared data—i.e. any change a user makes to their privacy settings should affect not only future shared data, but anything they have previously shared. In this way, a system that was not initially designed to allow fully informed consent could be adjusted to allow revocation of consent over time. However, such a capability requires the system's designers to have planned for adaption and future changes. And, given the interdependence of various software features, if a breach or unintended effect occurs, plans should include how data can be removed from the entire data supply chain—not just one company's servers.

One practice for mitigating the risks associated with data usage is coordination between stakeholders in webs of shared computing resources. This collective coordination and alignment on key standards is known as "federation" in the IT context. Standards for ethical and uniform treatment of user data should be added alongside existing agreements on uptime, general security measures and performance.[20] Federated identity management (and, as part of that management, single-sign-on tools) is a subset of broader discussions of federation. Identity management is another critical component of managing data ethics, so that stakeholders accessing customer data (as well as customers themselves) are verified to be permitted to access this data.

Communicating impact

As part of an investigation into a 2015 shooting incident in San Bernardino, California, The US Federal Bureau of Investigation (FBI) filed a court request for Apple's assistance in creating software to bypass security protocols on an iPhone owned by one of the perpetrators. Apple's public letter to its customers explaining its decision to challenge that request provides a glimpse into the complexity and potential risks. How society addresses matters such as these will be central to shaping 21st century ethics and law. Apple chose a very intentional, bold, and values-driven stance.[21] Perhaps most relevant to the issues of informed consent and intent to do no harm was Apple's choice to not only make a statement about its position and intention, but also to explain in layman's terms how the current security features function, how they would potentially be subverted by the proposed software, and what the future risks of having such software in existence would be, should the company comply with the FBI's request. In the words of Tim Cook, Apple's CEO, "This moment calls for public discussion, and we want our customers and people around the country to understand what is at stake."

This move is in stark contrast to the often lampooned iTunes EULA (see R. Sikoryak's "The Unabridged Graphic Adaptation [of] iTunes Terms and Conditions"), which may be seen as a small annoyance to users as they scroll past and accept without reading in order to access their music.[22] Like most EULAs, the dense legalese gives users a difficult time in determining the significance of any changes they need to "review" and "accept."

As users increasingly realize the importance and value of securing their data and sharing it selectively and with intent, brands that declare responsibility for educating their users about data security and use have an opportunity to build trust and loyalty from their customers. By focusing on more than just removing themselves from liability through processes that occur as a technicality in the user flow, and instead utilizing proactive measures (as Apple does by reminding users that location data is being used by apps) companies can establish themselves as industry leaders in ethical data use.

"Brands that declare responsibility for educating their users about data security and use have an opportunity to build trust and loyalty from their customers."

Building data literacy to earn trust and mitigate risk

To achieve informed consent on the part of data disclosers and maintain consent over time, organizations must ensure that employees and partners are informed of the goals for data use, and the ethical concerns and frameworks within which those actions must fall. This is called "data literacy"—a shared understanding of how data is disclosed, manipulated and processed—and it is needed throughout the organization.

At a minimum, a data literacy program should cover:

- What happens once data "leaves" the control of any one employee or user.
- The impossibility of a static enterprise architecture in the age of data interdependency (due to use of third-party APIs, data partnerships and common frameworks).
- Understanding of data at rest (stored data) versus data in motion (data being transformed into useful information by systems and people).

In the process of modeling potential uses for data, unspoken values will become apparent. If good feedback loops are in place, end users will be able to signal to developers where their values diverge from those of the developers, or where implementation does not bear out the intended result. Doctrine for data handling and management of consent needs to be incorporated not just at the edges of an organization's human decision-makers, but at the edges of its computing infrastructure as well (as embodied in the algorithms used in analytics or machine-learning processes).

Doctrines, which can be defined as guidelines for effective improvisation, can be used to achieve this requirement. Coined in business usage by Mark Bonchek, the concept is sourced originally from military contexts, where commanders need to empower the soldiers on the front lines to have rules of engagement which not only specifically proscribe or restrict their actions, but also give them sufficient information to make smart decisions in line with a larger strategy, even when not able to directly communicate with the command structure.[23]

Building data literacy

Wise leaders will attend to management of consent and prevention of harm through good design, seeking informed consent from users, monitoring and managing consent over time and creating harm mitigation strategies. And with data literacy programs in place in their organizations, embodied in clear doctrines, their teams and partners will be able to fulfill the promises companies have made to their users—both to avoid harm and to create new value.

Further discussion of implementing a doctrinal approach can be found in "Code of Ethics." The incorporation of values into machine teaching and learning is discussed at length in "Ethical Algorithms for Sense & Respond Systems."

Avoiding potential harm: Recommendations and strategies

100-day plan:

Over the next three months, these are the actions you can take to improve your informed consent practices and minimize potential harm:

Evaluate existing ethics codes that your business has agreed to follow. Consider whether they have sufficient guidance for data ethics. If not, host a design session to build a draft of your own Code of Data Ethics. Use the 12 guidelines for developing ethics codes as a guide. Coordinate with partners and suppliers to ensure their future ability to honor your new Code.

Build an operations plan for communicating and implementing your Code of Data Ethics by charting the roles that furnish, store, anonymize, access, and transform data on behalf of your customers.

Evaluate any informed consent agreements your organization offers for language that may be unclear and could lead to misunderstandings between your business and your customers. Begin to develop a plan to address these inconsistencies by simplifying language and clarifying intent around data use.

Pilot a data literacy training program for data scientists, technical architects, and marketing professionals. Use their feedback to refine a larger program for all employees.

Implement regular reviews of data-gathering techniques. Involve a diverse group of stakeholders and maximize transparency of the proceedings.

Perform a gap analysis of your company's current cybersecurity strategies that provide threat intelligence and other ways of discovering and automatically mitigating potential data breaches. Enumerate the potential harms that could impact your customers if your company mishandles or discloses data about them. Identify the organizations responsible for safeguarding against these missteps and communicate your findings with them.

Develop a training toolkit to teach your employees who interface with customers how to identify harms that occur through the use of your products. Priority rank the groups within your company who should receive the training with the group that responds to the greatest variety of situations as the highest priority.

Draft and launch a data literacy plan for ensuring shared understanding of data usage and potential harms throughout your organization, including partners and vendors.

365-day plan:

Over the next year, build on top of the short-term goals and scale improvements to include your entire company and ecosystem of stakeholders.

Gain support from your company's leadership team to ratify your Code of Data Ethics and start working with partners and vendors to integrate the principles into new agreements.

Roll out a data literacy training program for all employees.

Develop standard text to include in consent agreements that is easily understood and accessible. Consider altering the ways these agreements are shared with customers, how interactive they are, and how customers can revisit these agreements over the lifecycle of their relationship with your products, services, and brand. Instantiate varying degrees of these updates in a handful of agreements. Consent agreements should strive to communicate the scope of how data is collected, manipulated, and used as well as the value this data has for all of the stakeholders in the data supply chain who might come in contact with this data.

Now that potential harms have been enumerated, seek out instances of harm—first from existing feedback loops (e.g. call centers, customer service channels, surveys), and then create new methods for finding harms that fill gaps in existing feedback mechanisms. When unintended harms are discovered, document the incident in the form of a use case and share these findings with product owners and their managers.

Deploy your training toolkit to train groups of employees based on their priority ranking. These employees should understand how to identify, document, and internally report instances of harm. If appropriate, consider disclosing these reports publicly.

Align data use cases by product, interface, and data teams with the customers' use cases for sharing data in the first place.

Share the customer data-centric threat intelligence evaluation report with your CISO (or equivalent) and ask her to address the gaps your team found between what is currently in place and what a stronger posture might include.

References

1 Cassano, J. (2016, February 2). How Uber Profits Even While Its Drivers Aren't Earning Money. Retrieved June 1, 2016.

2 "…We've seen corporates play with even very young startups through this sort of "data diplomacy"…enabling an entrepreneur to get some limited access to data in order to test it out and create a product around it." Beyroutey J. and MJ Petroni (2013, September 17). Personal interview.

3 Open Letter to Facebook About its Real Names Policy. (2015, October 5). Retrieved April 3, 2016.

4 Osofsky, J., & Gage, T. (2015, December 15). Community Support FYI: Improving the Names Process on Facebook [facebook Newsroom]. Retrieved April 3, 2016.

5 Calvo, R. A., & Peters, D. (2014). *Positive Computing: Technology for Wellbeing and Human Potential.* The MIT Press.

6 Bonchek, M. (2013, May 3). Little Data Makes Big Data More Powerful. Retrieved June 1, 2016.

7 Seshagiri, A. (2014, October 1). Claims That Google Violates Gmail User Privacy. The New York Times. Retrieved June 1, 2016.

8 Kramera, A. D., Guilloryb, J. E., & Hancockb, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. PNAS, 111(29), 10779.

9 Goel, V. (2014, June 29). Facebook Tinkers With Users' Emotions in News Feed Experiment, Stirring Outcry. The New York Times. Retrieved June 1, 2016.

10 Schroepfer, M. (2014, October 2). Research at Facebook [facebook Newsroom]. Retrieved April 3, 2016.

11 Jackman, M., & Kanerva, L. (2016). Evolving the IRB: Building Robust Review for Industry Research. *Washington and Lee Law Review Online*, 72(3), 442.

12 Gewirtz, D. (2015, October 15). Europe to US: Stop storing our data on your servers (or else). Retrieved June 1, 2016.

13 Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009). A nutrition label for privacy. In Proceedings of the 5th Symposium on Usable Privacy and Security (p. 4). ACM. Retrieved March 3, 2016.

14 Kelley, P. G., Cesca, L., Bresee, J., & Cranor, L. F. (2010). Standardizing privacy notices: an online study of the nutrition label approach. In Proceedings of the SIGCHI Conference on Human factors in Computing Systems (pp. 1573–1582). ACM.

15 Usable Privacy. (n.d.). Retrieved March 3, 2016

16 PBS. (n.d.). Retrieved June 1, 2016

17 Tuerk, A. (2015, February 10). Take a Security Checkup on Safer Internet Day. Retrieved March 15, 2016

18 Kirchner, J. A., Surya Mattu, Jeff Larson, Lauren. (2016, May 23). Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks. Retrieved June 23, 2016.

19 The UX Of Ethics: Should Google Tell You If You Have Cancer? (2016, April 18). Retrieved May 7, 2016.

20 Federation (information technology). (2016, May 21). In Wikipedia, the free encyclopedia. Retrieved March 27, 2016.

21 Cook, T. (2016, February 16). Customer Letter. Retrieved February 17, 2016.

22 Sikoryak, R. (n.d.). iTunes Terms and Conditions: The Graphic Novel. Retrieved March 30, 2016.

23 Fussell, M. B. and C. (2013, February 20). Use Doctrine to Pierce the Fog of Business. Retrieved February 16, 2016.

Contact Us

Steven C. Tiell
Senior Principal—Digital Ethics
Accenture Labs
steven.c.tiell@accenture.com

MJ Petroni
Cyborg Anthropologist and CEO, Causeit, Inc.
mj@causeit.org

Jessica Long
Cyborg Anthropologist, Causeit, Inc,
jessica@causeit.org

Contributors

Scott L. David
University of Washington
sldavid@uw.edu

Harrison Lynch
Accenture Labs
harrison.lynch@accenture.com

About Accenture Labs

Accenture Labs invents the future for Accenture, our clients and the market. Focused on solving critical business problems with advanced technology, Accenture Labs brings fresh insights and innovations to our clients, helping them capitalize on dramatic changes in technology, business and society. Our dedicated team of technologists and researchers work with leaders across the company to invest in, incubate and deliver breakthrough ideas and solutions that help our clients create new sources of business advantage.

Accenture Labs is located in seven key research hubs around the world: Silicon Valley, CA; Sophia Antipolis, France; Arlington, Virginia; Beijing, China; Bangalore, India, Dublin, Ireland, and Tel Aviv, Israel. The Labs collaborates extensively with Accenture's network of nearly 400 innovation centers, studios and centers of excellence located in 92 cities and 35 countries globally to deliver cutting-edge research, insights and solutions to clients where they operate and live.

For more information, please visit www.accenture.com/labs.

Data Ethics Research Initiative

Launched by Accenture's Technology Vision team, the Data Ethics Research Initiative brings together leading thinkers and researchers from Accenture Labs and over a dozen external organizations to explore the most pertinent issues of data ethics in the digital economy. The goal of this research initiative is to outline strategic guidelines and tactical actions businesses, government agencies, and NGOs can take to adopt ethical practices throughout their data supply chains.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 375,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

Learn more: www.accenture.com/DataEthics

This document makes descriptive reference to trademarks that may be owned by others.

The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.