Data Science and Designing for Privacy

Michael Falgoust

Abstract: Unprecedented advances in the ability to store, analyze, and retrieve data is the hallmark of the information age. Along with enhanced capability to identify meaningful patterns in large data sets, contemporary data science renders many classical models of privacy protection ineffective. Addressing these issues through privacy-sensitive design is insufficient because advanced data science is mutually exclusive with preserving privacy. The special privacy problem posed by data analysis has so far escaped even leading accounts of informational privacy. Here, I argue that accounts of privacy must include norms about information processing in addition to norms about information flow. Ultimately, users need the resources to control how and when personal information is processed and the knowledge to make information decisions about that control. While privacy is an insufficient design constraint, value-sensitive design around control and transparency can support privacy in the information age.

Key words: data science, privacy, value-sensitive design, autonomy

1. Introduction

We call it “the information age,” because the integration of personal computers into everyday life has changed one major thing. The inhabitants of the information age have more access to more information, all facilitated by the revolution in digital computing. Computing contributes to the revolution in information access in two ways. First of all, even the earliest digital computers performed algorithmic computations faster and more efficiently than human operators. As such, the ability to process data into usable forms or insights, such as in statistics, is greatly enhanced. Secondly, enhanced data storage and retrieval facilitates the accumulation of information, ultimately making more data available for processing. The intersection of faster processing and high-capacity storage brought “Big Data” into

Michael Falgoust, University of Twente, Drienerlolaan 5, 7522NB, Enschede, The Netherlands; mfalgou@tulane.edu.
focus. For the most part, “Big Data” refers to information processing with large and complex data sets that strain the capability of traditional modes of processing. All of these advances have made data science, the study of more effective means to extract knowledge from data, a highly visible discipline in the information age.

Privacy concerns arise from the fear that the aggregation of publicly available information can reveal private information when processed through the “black box” of data science. There is a fear that our disparate data “knows” more about us than we know about ourselves, that we will be classified and judged based on how our data is processed rather than what we do. If private information can be extracted from publicly available data, maintaining a robust private sphere becomes impossible.

All of the above issues have been expressed by leading scholars on privacy in the information age. Responses to these concerns have varied, from those who embrace the loss of privacy as a kind of liberation to privacy engineers focused on designing privacy into various information systems such as cloud computing platforms, social networking services, and email providers. Given the discussion of data science and Big Data above, designing for privacy must include both the protection of private information from interception and the derivation of private information through sophisticated information processing. As a design goal, “privacy” is too coarse-grained to constrain the concerns about privacy raised by data science. To make this point clear will require analysis of the different moral assessments of privacy loss as opposed to privacy violation. I contend that while the post-privacy stance is unacceptable from a moral perspective as it deprives individuals of their autonomy, the pro-privacy stance needs to define more specific design goals and provide a normative account of privacy loss through information processing. A refinement of Helen Nissenbaum’s Contextual Integrity account of privacy to include norms of processing as well as norms of flow may be sufficient to provide the latter. Drawing connections between the norms of processing and the underlying moral value of privacy should offer some insights or general suggestions on more refined design principles that favor of privacy. Two examples, transparency and user control, will be highlighted by the analysis.

2. Finding Meaningful Patterns and Maintaining Privacy

Data science is something of a hybrid of engineering and science. Insofar as the focus of data science is the development of new methods to detect meaningful patterns in large data sets, it is the domain of engineers. Insofar as engineering new tools and methods must inquire into the deep structures of statistics and computer science, it is a branch of information science. Successful data science requires
both an understanding of the technological capabilities of information systems as well as an understanding of the “behavior” of information, complex systems, and network theory.

With all of this in mind, let us understand data science as the pursuit of more effective means of discovering meaningful patterns in data sets. Data science drives the success of Google and other “Big Data” industry titans (Oracle, Yahoo, IBM, etc.) by enabling firms to provide valuable informational goods to users and commercial clients. Many of these firms (notably IBM, Oracle, and Google) also contribute significantly to the development (both initial and ongoing) of tools and techniques for analysis. The achievements in this field are fascinating in part because information not visible or expected at the level of small-scale data sets can be revealed through processing very large sets with surprisingly simple algorithms.

While enhanced access to information opens up new scientific, technological, and economic possibilities, concerns about privacy also arise. To advance data science, researchers need data sets. As data transmitted across networks is notably “greased,” harvesting the digital traces of user activity offers a plentiful supply of data (Moor 1997). As social networks expand, millions of users are indexed and tracked. While their personal data is usually “anonymized” by removing identifying information, data scientists have demonstrated that anonymous data can be re-identified through correlation across data sets (Brunton and Nissenbaum 2011). In addition to social networks, search engines track connections across the Web and store queries to refine future results.

Inexpensive monitoring systems allow for gathering large volumes of information in public places and others centers of activity. Movements of individuals, financial transactions, and purchasing patterns can be logged and processed to extract useful insights. Online retailers track shopping and purchasing behavior to refine their offerings to customers. Loyalty cards offered by many grocery stores allow retailers to track purchasing patterns. Enhanced ability to analyze information makes our society hungry for more data, inspiring new methods to acquire information from users and complicating efforts to maintain some sense of privacy (Brey 2005).

Data collection methods excite a wide range of privacy concerns, already discussed in computer ethics and privacy scholarship. One way to protect privacy in the information age is to find ways of limiting access to personal data. Advocating for data minimization, limiting retention of personal data, and obfuscating private data aim to prevent the exposure of private information. While this is an important concern, the gathering of data only partially addresses privacy concerns.
Since data can be revealed through analysis, in addition to being gathered or aggregated, these strategies do not fully contain privacy risks.

3. Privacy and Design

It is tempting to address some of the privacy issues through the lens of value-sensitive design, a design approach that emphasizes taking moral values as design constraints (Friedman 1996). By taking privacy as a design concern, engineers can limit the harms of information access while preserving the benefits. This kind of thinking informs the Privacy by Design (PbD) approach to information systems (Cavoukian 2011). Value-sensitive design is an important field of study for navigating the ethical challenges of the digital age. While PbD is well-intended, the imperative to include privacy as a design concern does not offer any concrete guidance for engineers (Gürses, Troncoso, and Diaz 2011). To be effective, value-sensitive design requires sophisticated understanding of the relevant technology and clear identification of values justified by normative ethical theory. The technology of concern here is data science, the increasingly important study of generating knowledge from large data sets. Unfortunately, the aims of data science and a coarse-grained norm in favor of privacy are inconsistent. Where privacy entails controlling access to information about oneself, data science enhances the generation of personal data through analysis.

In an age of total information access, privacy must be understood as a dynamic, multifaceted concept. There is an increased emphasis on informational privacy over or in addition to privacy as obscurity or concealment. With so much information available from various sources, contemporary privacy scholars emphasize control over private information and how private information moves across contexts. Herman Tavani prefers to cash out privacy in terms of managing access to information and exercising some control over how it moves beyond grants of access (Tavani 2007). The somewhat more influential account of Nissenbaum frames the problem of the information age as “privacy in public” where privacy must be understood in terms of information flow between contexts. Since fully concealing private information is not possible, and in fact not desirable in some transactions, such as those between medical professionals, Nissenbaum cashes out privacy as contextual integrity (CI). For Nissenbaum, privacy must be understood in terms of “norms of flow” that describe how information should move (or not) across contexts (Nissenbaum 2009). Both Tavani’s and Nissenbaum’s accounts share an emphasis on the subject of privacy maintaining control over personal information.
On the other hand, the development of more sophisticated data science enables the extraction of insightful patterns from data sets. Much fascination is focused on “Big Data”—the use of large, aggregated, disparate, and at times incomplete data sets—made possible by advances in processing power, memory, and storage capacity. With larger and more disparate data sets available, surprising correlations and predictions can be revealed through analysis. This is noteworthy because private information can be discovered through analysis rather than directly accessed from some licit or illicit flow.

Consider again the aim of data science: effective identification of meaningful patterns in large data sets. One should imagine that a completed data science would enable accurate detection of patterns in impossibly large unstructured data sets and locate correlations across many and diverse data sets. From a diverse and incomplete soup of data points, an idealized data scientist would be able to extract specific, true, and relevant information. Our idealized scientist could enter a single known point along with a query, and her system could locate all relevant correlations or patterns, picking out the correct answer to the query with a high degree of accuracy. For instance, if she were expecting the arrival of a keynote speaker for her conference but only knew the speaker’s arrival time, the data scientist could use her system to isolate all collisions with that arrival time to determine the mode of transportation, the operating firm, and destination terminal. Her system could accurately calculate the time required to exit from the transportation, retrieve baggage, and walk to the pick-up location, enabling the data scientist to know when to retrieve her keynote speaker.

This image of a completed data science does not lie in a terribly distant future. Current wisdom indicates that with no more than three data points—gender, birthday, and postal code—any individual can be identified (Sweeney 2000). The completed data science outlined above may require only one vital statistic, restricted by the content of the query alone. We do not yet know the full limits of data science, but the ends that data scientists work toward include needing less (and less specific) information to extract meaningful insights. The development of data science then works directly against design constraints around privacy as data science cannot develop without opening new avenues to discover private information without breaking norms of flow. These considerations show that a more sophisticated approach is needed.
4. Conflicting Maxims

To unpack the concern about privacy outlined above, it is helpful to frame data science and Privacy by Design as formal imperatives. The aims of any science can be framed as a command that defines the relevant field of research. With regard to data science, the maxim can be framed: “Data scientists should design and develop the means to extract as much knowledge as possible from available data.” Formalizing the maxim in this way reveals the fundamental aims of the discipline, the values expressed by the line of inquiry. Since resulting innovations will be embedded with these values, the maxim provides the basis for ethical assessment of a research field and its technologies. Evaluating the maxim allows us to evaluate the potential moral impact of a science.

Applying privacy as a design constraint can be framed in a maxim as well: “Data scientists should develop tools that respect individuals desire to control and restrict access to private information.” While neither the privacy maxim nor the data science maxim are problematic alone, they are inconsistent with one another. The ability to extract knowledge from available data entails the loss of the private domain. Tracking an individual’s habits in public space, aggregating the data, and picking out correlations enables the construction of private information from public information. As data science improves, the ability to reliably identify patterns improves, making it more difficult for users to control data about themselves. Maintaining a protected domain, free from observation or interference, becomes impossible.

While data science promises (and delivers) many benefits for clinical medicine, machine learning, and the social sciences, the enhanced ability to identify patterns entails increased difficulty in protecting privacy. The ICT infrastructure makes data collection and analysis possible through a distributed network of intermediaries. Everyone who uses the Internet leaves “digital footprints” as their online activity is passed through many electronic hands. Internet traffic is routinely logged for security and troubleshooting purposes (if nothing else). Everyone who lives in a networked society (and even some who do not) have a digital presence composed of activity logs, database entries, and user-uploaded content. To locate a specific person, one need only identify the subject’s digital presence, typically through correlation with known data points (e.g., name and location, name and birthday, picture and school attended). Such searches are fairly simple to perform using Google or other search engines. If an agent wants to remain entirely unknown, she has few options as she may have a digital presence composed of school alumni lists, telephone directories, or professional society membership rolls. Data
science makes finding things easy, even when those things are people, so applying a course-grained notion of “privacy” as a design constraint renders data science impossible. Nevertheless, a more fine-grained approach to privacy can yield specific design constraints that make a privacy-supporting data science possible.

5. Analysis-based Exposure

A data scientist utilizing the tools and methods of the completed data science imagined above may not be able to locate any individual with complete certainty, but may nevertheless be able to match unknowns to particular individuals with a high degree of probability approaching complete accuracy. The absence of private information would prove no obstacle because publicly available information provides sufficient anchors for a sophisticated analysis, filling in the “private” gaps with probabilistic projections informed by common and known patterns of correlation.

Consider a recent case involving the American retailer Target. Like many retailers, Target monitors purchases and sends coupons to frequent customers. Sophisticated analysis of purchasing patterns allows Target to send coupons tailored to customer’s habits and in anticipation of likely purchases. As reported in Forbes, a family in Minnesota received coupons directed at expectant parents, addressed to the family’s teenage daughter. While news about the daughter’s pregnancy came as a shock to her parents, Target’s analysts had developed a metric for determining the probability that a customer is pregnant given her purchasing patterns. The metric accurately predicted the daughter’s pregnancy based on minor variance in her purchases (Hill 2012).

There are two interesting features of this particular case. First, Target’s data analysis is current technology, not idealized or completed data science. The current state of play in data science enables predictions and insights that are truly staggering. In addition, Target did not violate the customer’s privacy in any traditionally understood fashion. While customers may have been surprised to learn about the extent of Target’s monitoring, at no point did Target obtain sensitive information directly through any illicit means. Instead, the analysis was carried out using the retailer’s own sales records, deriving patterns of correlation from available data. Without any invasive collection of information, Target’s analysts can accurately predict facts about their customers.

What needs to be understood about value-sensitive design in data science is that information systems cannot distinguish between private information and public information unless known data points are somehow flagged. Analytic software is designed to locate data points, nothing more. An isolated data point is not intrin-
sically imbued with status as private or public. Information must be designated as private for an analytic application to be “aware” of privacy concerns. If I create a database of medical information, I can design the database so that certain fields are only available to certain users. Nurses may be able to see when a patient was last admitted or discharged, but not diagnostic information available only to attending doctors. This kind of restriction is possible because the database consists of definite facts that are categorized according to access permissions. In other words, information about privacy is entered along with the data as the database is populated.

If we take our medical database and extract only publicly available information (perhaps only the patterns of admission and discharge of patients), data analysis would likely be able to draw some meaningful conclusions about the hospital, the staff, or the patients. Given the success of Target’s analysts, we might expect that some of these predictions would be accurate, likely resulting in gaining private information without any formal violation of privacy. Since the resulting predictions are not known before the analysis takes place, there is no way to designate that some predictions will concern private information to filter them out of the results. The system will simply produce predictions according to its programs.

If one argues that the operator should take care in setting the parameters of the analysis, we must again recall the content of the predictions is unknown before the analysis takes place. A data scientist can conduct an analysis and be surprised at the results. She may take care in restricting the scope of an analysis in the interest of avoiding uncovering private information and uncover it because private information is revealed within the scope of her restrictions. We employ information systems because we are incapable of conducting the analysis ourselves. We design the statistical theorems and select the data sets and analytic metrics, but we cannot know the results until the analysis is performed.

6. The Sherlock Question

There are two avenues of objecting to the privacy concerns outlined above. From a post-privacy perspective, one could argue that abandoning efforts to uphold privacy in data science simply slows down an inevitable drift toward a total information society. We can give up on privacy or data science, but the contradiction raised above indicates that we cannot maintain both. Given the integration of computers and information services into government, professions, and education, we should accept that privacy is or will shortly be lost as data science develops. We will call this the Post-Privacy Objection.
In addition, one might reasonably question whether data science violates privacy in any coherent sense. Accounts of privacy must distinguish between privacy loss and privacy violation. When an agent discloses something about herself to a friend, she has lost some privacy, but since she discloses willingly, her privacy has not been violated. A privacy violation entails some illicit act of discovery, or in Judith Jarvis Thomson’s phrase “a right that certain steps not be taken to find out facts” (Thomson 1975). Given that data science could use publicly available data to infer private information, one might argue that there is no illicit discovery. Nissenbaum’s Contextual Integrity account of privacy provides a framework for understanding privacy violation alongside disclosure of information, but privacy violation is framed against norms about how information should flow across contexts.

In the data science case, information does not flow; it is inferred from (licitly) available data. Furthermore, we might call into question whether the insights of data science are as robust as we take them to be. An accurate prediction (or projection) may make one feel that one’s privacy has been violated, but inaccurate predictions raise no such concerns. If insights from data science do not count as knowledge, or as “facts” in Thomson’s words, it may be incoherent to refer to a privacy loss. As such, one may object that the concern about data science is really a non-concern, the result of a moral panic, or a misunderstanding of what data scientists do and how data science works. We will refer to this as the No-Violation Objection.

6.1. Post-Privacy and Self-Presentation

Given the fundamental conflict between the data science that drives the information society and the privacy that we hold dear, one might wonder why we do not work toward a post-privacy moral landscape. On an instrumentalist account of privacy, privacy is valuable as a prerequisite to other goods such as autonomy or self-reflection (Moor 1997). If we value privacy because it protects us from interference or the potential for external judgment, then in a world where there are no such consequences, there would be no need or value for privacy. If we consider the range of benefits made available by privacy-compromising technologies, or advantages to research that could be gained by shedding attachment to privacy, the trade may even be considered quite attractive (Majoo 2014).

A post-privacy society seems especially viable given the reduction in privacy coincident with the rise of the information age. Through social networking, public databases, and sophisticated search engines, judgments about compliance with social norms could be tempered by the knowledge that an accuser’s own deviations are just as public as those of any accused. Individual quirks and eccentrici-
ties can be readily exposed and even celebrated rather than ridiculed. One might argue that diminished privacy serves as a benefit, bringing out all of the wonderful cacophony of individual differences to show each one of us that while we are all unique, we are the same in our differences. None of us should be judged for our quirks, whatever they may be, because we all of us possess quirks that would invite ridicule or embarrassment. If a norm against such judgments becomes dominant, we might lose the fear of exposure that motivates our valuing privacy.

Unfortunately, this vision of the post-privacy society fails to recognize the importance of control connected to our sense of privacy. An instrumental account of privacy that vests the value of privacy in desires (or simply norms) against interference only captures a subset of the most immediate benefits secured by the private sphere. Certainly, agents desire privacy because the private sphere allows them to do as they wish without the intrusion of external norms or even the fear of such intrusion. In addition to relief from that fear, privacy also allows agents to control the distribution of information about themselves, allowing them to control their self-presentation (Manders-Huits 2010).

The creation of the self-identity, especially the identity as a moral agent, must take place within a context where the agent herself is in control. Autonomy is a key prerequisite for moral agency, and when we lose the ability to control information about ourselves, we lose the ability to present ourselves according to our own self-conception (Shoemaker 2010). Without privacy, facts about an individual are (and/or can be) presented without the reflective understanding of the agent herself. Her facts are, as it were, laid naked before an audience, with no guidance or direction, no dressing or intentional presentation. The agent cannot fully express herself because the self perceived by others is not channeled through her own self-understanding.

We might put these issues more vividly by considering some emotivist arguments about privacy. While a complete explanation of privacy violation must include more than appeals to the feeling of being violated, one should expect the victim of a moral injustice feels outraged (Roeser 2006). Emotional reactions to privacy violations do not capture the extent of the violation, but they do track the expectations of the victim regarding what should be public knowledge. At worst, an agent’s feeling that privacy has been violated indicates the intended context of the relevant information may have been compromised (Nissenbaum 1998).

Consider the fictional character Sherlock Holmes. Sherlock is a master of deductive logic and the art of observation. As such, when Sherlock trains his attention on a subject, he can extract information about the subject that the subject
Data Science and Designing for Privacy

does not intentionally disclose. On his first meeting with Dr. Watson, Holmes swiftly concludes from Watson’s dress, bearing, and skin tone that he is a military doctor recently returned from Afghanistan. Watson never discloses his profession or history deliberately, but Sherlock nevertheless “reads” those facts by carefully observing Watson. Does Sherlock invade Watson’s privacy?

On traditional account, he does not, because Sherlock does not invade or intrude into Watson’s private space. Nevertheless, one would likely be unsurprised if Watson reported that Sherlock’s knowledge was uncanny (or, in contemporary parlance, “creepy”) because Sherlock nevertheless arrived at true beliefs about Watson that Watson did not intentionally disclose. While Watson’s surprise in and of itself does not demonstrate that Sherlock has invaded his privacy, the sentiment does signal that there is some felt-sense of invasion in Sherlock’s knowledge. If Sherlock has invaded or intruded on something other than Watson’s privacy, what is it?

In their conversation, Sherlock does take something away from Watson: the ability to introduce and present himself. This ability is something we often readily give away when seeking connections through intermediaries, but it is notable that we do this by choice. We reserve for ourselves the right to identify and define ourselves to others (Shoemaker 2010). When Sherlock deduces Watson’s history, he prevents Watson from presenting himself in his own narrative, from presenting his identity as he sees it. Watson’s surprise is much like common reactions to online behavioral advertising, a creepy sense that someone unknown is watching and accurately deriving information known only to oneself (Ur et al. 2012).

One might imagine that in the post-privacy society, Watson’s feelings would be considered misplaced. Along with a norm against judging people for their quirks, the post-privacy society would embrace an expectation that others know more about you than you have disclosed. A fully post-privacy Watson would have no such reaction to Sherlock because Sherlock’s demonstration would conform to expectations regarding knowledge about the self. Were that to be the case, we would nevertheless find ourselves consistently prevented from telling our own stories, from presenting ourselves from our own perspective. The Post-Privacy Objection fails to account for the sense of control that privacy provides. An agent with no informational privacy, no control over the distribution of information about herself, has diminished autonomy in self-presentation. The agent loses the sense of herself that she gains by crafting and telling the narrative of her own life.

Taking away the risk of interference or judgment does not alter the importance of privacy for allowing us to control self-presentation. Without any social or legal consequences for disclosure of quirks, medical conditions, or sexual orientation,
individuals in the post-privacy society lack an important component of agency. The diminished sense of autonomy over self-presentation (and as a result narrative identity) disassociates agents from themselves. The narrative of a person’s life would be no longer self-created, connected to a sense of future self that allows for moral reasoning. At best, such an agent would be unable to give full consent to losing privacy because consent requires agency with regard to decisions about one’s future (Korsgaard 1989).

6.2. Violation, Loss, or Other?

The Sherlock case as described above also offers a way of responding to the No-Violation Objection. Under Nissenbaum’s CI account of privacy in that, where Sherlock violates privacy, he must violate something other than the norms of flow that Nissenbaum describes. Sherlock does not illicitly gain information about Watson from some definite source. Instead, he constructs the information about Watson through an analysis of what must be described as readily available information. If Watson’s privacy is violated, the violation must be described in terms of a norm of processing rather than the norms of flow that Nissenbaum describes. One might be tempted to deflect this concern with resort to a well-understood distinction between privacy violation and privacy loss. In the classic case, a couple’s privacy is lost when the wind blows open a door, rendering their argument audible to the neighbors, but it is not violated because there is no intention to gain the relevant information (Moore 2003). If we take intentionality to be the hallmark of violation rather than loss, then there should be no violation in terms of processing norms. Nissenbaum’s arguments clearly resist this conclusion, but the norms of flow that structure her CI account of privacy do not provide a framework for explaining “deductive” violations where there has been no illicit flow.

Nevertheless, the analysis of self-presentation presented above shows that there is a cost to autonomy when privacy is lost through processing. This loss is entirely parallel if not identical to the autonomy cost that accompanies a violation of flow. If I hire a private investigator to discover facts about a potential business partner, intending to confront the partner with some of those facts on first meeting, I have deprived the partner of the opportunity to present herself as she would prefer. What makes this case different from “Google-stalking” a person before first meeting (or, in a very usual case for academics, before a conference or job interview)? In Google-stalking, the information flows from public channels rather than the person, but this does not in turn differ from learning of a person’s institutional affiliation through a news story. In both cases, the information is public and
available. An agent may expect her institutional affiliation to be known because it is readily available through a casual search. What is of concern with norms of processing, as in the PI case, is deriving personal information indirectly or illicitly. The private investigator violates a norm of flow by searching through discarded paperwork, covertly following the subject, or questioning known associates on deceptive pretexts. In the Sherlock case, information not readily available is revealed through analysis of what is readily available. As such, Watson’s surprise highlights that Sherlock’s (accurate) guesses fall outside of the range of Watson’s expectations. The private investigator and Sherlock both deprive the relevant data subject of their ability to present themselves. As such, it may be necessary to conclude that, rather than intentionality on the part of the observer, the expectations of the subject determine whether we need to describe a situation as a privacy loss or a privacy violation. If so, one must conclude that there are norms of processing in addition to norms of flow that define privacy violation under a CI account of privacy.

With a norm of processing in view, the No-Violation objection can be readily answered. A privacy violation in data science can be framed in terms of a subject’s expectations around how the data will be used and what can be derived from it. Where the subject’s expectations are exceeded, a privacy violation has occurred. In this regard, privacy could be strengthened through implementing a standard of consent that is both active (opt-in) and informed regarding data use. In addition to the need for control evoked by responding to the Post-Privacy Objection, responding to the No-Violation Objection reveals a need for transparency of data processing.

7. Solutions in Technology: Values We Can Design

Given the insights above, privacy concerns are too coarse-grained to be accounted for in data science design. Informational privacy entails a complex of controls held by an agent over her personal information. As in the above example, one can design a database that incorporates access permissions, but fails to protect information from data mining. By nature, innovations in data science will make information more difficult to conceal, easier to extrapolate from available data. Designing for privacy must be cashed out in terms of values that are both relevant to data science design and supportive of a robust right to privacy.

Responses to the objections outlined above show that even in a society without consequences for self-regarding action, the loss of control over self-presentation remains a concern. Some control over personal information is required for an agent to craft and take ownership of a narrative identity. Framing informational privacy as contextual integrity provides further support to the importance of control. Under
a contextual integrity account, violations of privacy are most clear when personal information escapes the intended scope of revelation (Nissenbaum 2004).

To maintain privacy, users need control over the distribution of their personal information. Users take control over their self-presentation in part by defining different relationships through differing patterns of behavior (Reiman 1976). Social networking platforms map patterns of associations among users, making it possible to connect user information across contexts. The software that allows service providers to identify users and manage access to services makes it more difficult for those users to manage their own self-presentation (Manders-Huits 2010). These concerns could be mitigated with default privacy settings that require the user to authorize all information sharing and directly consent to making personal data available for processing. Active “opt in” style consent should be a norm for all information requests between a user and a service provider (Costa and Poullet 2012).

General norms in favor of user control over information would result in more sensitivity to privacy concerns. The privacy concerns raised by the information age originate in the sense that users lose control over disclosure. A profile can be created for any individual by aggregating public data from different sources. A user cannot control the narrative of her identity without competing with the narrative derivable through data mining. If there is a presumption that users will want to actively control the distribution of personal information, some sense of control can be established, and this sort of privacy concern could be mitigated. As such, design norms in favor of user control over personal information would support user autonomy, one component of privacy.

The sense of control can be augmented with design norms in favor of transparency. For users to feel fully in control of their information, they must also know more about the risks of sharing information. A user cannot effectively offer or withdraw consent without knowing how her consent will impact privacy. To support autonomy robustly, users need to be capable of informed consent. Knowledge about how personal data is collected and used supports more informed decisions. Unfortunately, typical graphical user interface (GUI) design conventions occlude many basic functions from the user. While making the system architecture less visible reduces the learning curve for ICT, users become proficient with the interface rather than the system itself. As a result, there is a substantial knowledge gap between specialists and non-specialists, especially with regard to information security.

Transparency-sensitive design would favor GUI designs that expose the user to the functions and relationships among the operating system, the hardware, and
the various applications and interfaces that compose the system. Making the user more aware of system logs and communication protocols would also make the user more aware of potential vulnerabilities in email and web browsers. Ideally, GUI design should reward curiosity and encourage discovery, raising the user’s understanding of the device and providing opportunities for the user to explore the technology. More informed users can exercise more control by implementing effective security measures and forming warranted judgments in their relationships with information vendors.

One should also note that a transparency-sensitive design norm should be understood as a shift in design conventions. This is the central concern of the GUI-design argument offered here. Current GUI design conventions do users a disservice by limiting opportunities for discovery, opportunities to close the knowledge gap between users and developers (or between non-specialists and specialists). While some division of labor is both desired and required for complex societies, individuals must retain the ability to make informed choices where such decisions may have an impact on autonomy in a larger sense. Considering the importance of information in complex societies, individuals must have access to certain kinds of information to form and act on rational plans of life (van den Hoven and Rooksby 2008). The arguments offered here show that there is a specific component to distributive norms about information. With such substantial knowledge gaps, even requirements of active “opt-in” consent accomplish little as users are often uninformed about to what, exactly, they consent and how it might affect their privacy. Where ICT system design has a specific impact on individual autonomy, users must have opportunities, and possibly encouragement, to become more informed about the operation of these systems in the interest of supporting more informed choices. Where current GUI design conventions do not support opportunities for discovery, the distributive principle cannot be satisfied.

8. Concluding Remarks

There is no doubt that information technology and data science radically transformed even highly developed economies. The market for informational goods and the ability to trade individual data for useful services was unimaginable before the digital revolution. Every major social, economic, or political upheaval comes with its practical and moral challenges. The mastery of information, gaining knowledge about our world without losing control of ourselves, will likely be regarded as the defining challenge of the information age. Abandoning privacy and embracing the unrestricted information flows may be tempting, but losing control
over creating our own narrative of ourselves means that we sacrifice something crucial to personhood, leaving us with only very hollow potential for well-being.

Fortunately, the call for value-sensitive design sounds during a period of rapid innovation, another characteristic feature of the information age. Opportunities to build enduring values into the information age are present, but they must be seen clearly and grasped firmly. In this regard, the most important insight offered here is a more fine-grained analysis of what privacy-sensitive design must mean with regard to data science and the information processing and management systems that arise from it. For the purpose of information systems, attending to privacy alone is insufficient and inefficient as superior data science can show the way to circumvent any simple privacy protection, as shown by the re-identification of anonymized data. Nevertheless, there is a way forward for both data science and privacy by attending to the need for control and transparency, two values that support privacy indirectly. By placing users in control of their information, providing clear descriptions of how it will be used, and situating users in systems that invite further learning and understanding, users gain a significant measure of autonomy. Embedding sensitivity to these values will require distributed effort on many layers of the relevant technology, from the user-facing GUI to the “back end” processing systems. Nevertheless, the value of privacy will endure as long as personhood and autonomy are valued, so humanizing the information age must be a cardinal concern.

References


