Addressing Conceptual Gaps in Big Data Research Ethics: An Application of Contextual Integrity

Michael Zimmer

Abstract
The rise of big data has provided new avenues for researchers to explore, observe, and measure human opinions, activities, and interactions. While scholars, professional societies, and ethical review boards have long-established research ethics frameworks to ensure the rights and welfare of the research subjects are protected, the rapid rise of big data-based research generates new challenges to long-held ethical assumptions and guidelines. This article discloses emerging conceptual gaps in relation to how researchers and ethical review boards think about privacy, anonymity, consent, and harm in the context of big data research. It closes by invoking Nissenbaum’s theory of “privacy as contextual integrity” as a useful heuristic to guide ethical decision-making in big data research projects.

Keywords
big data, research ethics, consent, privacy, contextual integrity

Introduction
We have entered the era of big data. We can now access petabytes of transaction data, clickstreams and cookie logs, media files, and digital archives, as well as data from social networks, mobile phones, and wearable devices. These data are growing exponentially, as is the technology to extract insights, discoveries, and meaning from them. To date, computer scientists, mathematicians, and statisticians working in information-rich industries have largely dominated this new data science. But the tools for working with big data are improving fast, and a much wider range of sectors—including health care, manufacturing, education, and government—are now in pursuit of the value of data-driven decision-making that big data promise.

Furthermore, big data captured from Internet and social media platforms have emerged as a rich terrain for engaging in scholarly research and experimentation—in both academic and commercial environments—often yielding novel results while also generating considerable controversy. For example, a decade ago, AOL released over 20 million search queries from 658,000 of its users to the public in an attempt to support academic research on search engine usage, resulting in considerable controversy. For example, a decade ago, AOL released over 20 million search queries from 658,000 of its users to the public in an attempt to support academic research on search engine usage, resulting in individual users being re-identified based on an analysis of their search activities (Barbaro & Zeller, 2006); in 2008, Harvard researchers released the first wave of their “Tastes, Ties, and Time” data set comprising 4 years’ worth of complete Facebook profile data harvested from the accounts of an entire cohort of 1,700 college students, spurring concerns about confidentiality and the lack of consent (Parry, 2011); in 2014, academic researchers, in partnership with Facebook, sparked an uproar when they altered the emotional content within the News Feeds of nearly 700,000 Facebook users to study the impact on users’ mood (McNeal, 2014); and in 2016, a group of Danish researchers were roundly criticized after they publicly released a data set of nearly 70,000 users of the online dating site OkCupid, including usernames, age, gender, location, and kind of relationship (or sex) they are interested in, personality traits, and answers to thousands of personal profiling questions used by the site (Zimmer, 2016b).

In each of these cases, researchers hoped to advance our understanding of a phenomenon by analyzing—and often publicly sharing—large data sets of user information they
considered freely available for research purposes. Yet, in each case, controversies about the ethics behind such big data research projects quickly surfaced. Many of the basic tenets of research ethics—such as protecting the privacy of subjects, obtaining informed consent, maintaining the confidentiality of any data collected, and minimizing harm—appeared to be deficient in the researchers’ methodological protocols. And, while awareness of the unique ethical dimensions of Internet-based research has been increasing over the past two decades (see, for example, Buchanan, 2010; Heider & Massanari, 2012; Jones, 1998; Markham & Baym, 2008; Zimmer & Kinder-Kurland, 2017), research ethics expert Elizabeth Buchanan (2016) argues we are entering a new era of Internet-based research centered on big data, and, unsurprisingly, debates over the ethics of big data research flourish (Leetaru, 2016; Zhang, 2016).

In his foundational essay, “What is Computer Ethics?,” James Moor (1985) notes how the malleable nature of computer technology—the ease at which it can be shaped and molded for use in a variety of unexpected ways—will transform “many of our human activities and social institutions,” and will “leave us with policy and conceptual vacuums about how to use computer technology” (p. 272). Thus, Moor (1985) argues, we are left with little guidance on how to address the new ethical dilemmas that inevitably arise with the increased use of computer technology:

A typical problem in Computer Ethics arises because there is a policy vacuum about how computer technology should be used. Computers provide us with new capabilities and these in turn give us new choices for action. Often, either no policies for conduct in these situations exist or existing policies seem inadequate. A central task of Computer Ethics is to determine what we should do in such cases, that is, formulate policies to guide our actions. (p. 266)

Today, we are confronted with innumerable policy vacuums and conceptual gaps triggered by big data’s astonishing ability to transform “many of our human activities and social institutions,” far beyond what Moor envisioned with computing technology 30 years ago.

Attempts to fill the policy vacuums and clarify the conceptual gaps created in the wake of big data research are in the nascent stage, originating largely from a set of concerned computer scientists, social scientists, and information ethicists (see, for example, Bowser & Tsai, 2015; Buchanan & Zimmer, 2016; Metcalf & Crawford, 2016; Vitak, Shilton, & Ashktorab, 2016). This article will help push forward the growing discourse on the ethics of big data research by disclosing critical conceptual gaps that often hamper how researchers and Institutional Review Boards (IRBs) think about informed consent, privacy, personal information, and harm in the context of big data, focusing on the 2016 release of OkCupid profile data by Danish researchers. To attempt to address these conceptual gaps in how researchers address the ethical issues of consent, privacy, and harm, this article invokes Nissenbaum’s (2004, 2010) theory of “privacy as contextual integrity” as a useful heuristic to guide ethical decision-making in big data research projects. Rather than prescribing universal rules on ethical big data research, this article will instead reveal how approaching research ethics through the lens of contextual integrity will empower researchers to be more attentive of the normative bounds of how information flows within specific contexts. By striving to maintain the contextual integrity of those information flows, we can start to resolve the conceptual gaps that plague big data research ethics.

Core Principles of Research Ethics

Research ethics attempts to provide guidelines for the responsible conduct of research, typically focusing on research involving human subjects. Numerous global bodies have enacted ethical guidelines for the protection of human research subjects, including the Canadian Tri-Council, the Australian Research Council, The Research Council of Norway and its National Committee for Research Ethics in the Social Sciences and Humanities, the United Kingdom’s National Research Ethics Service, and the Forum for Ethical Review Committees in Asia and the Western Pacific (FERCAP). In the United States, the Department of Health and Human Services maintains a set of basic regulations governing the protection of human subjects (codified in 1974 within regulations 45 CFR 46), complemented by the publication of the “Ethical Principles and Guidelines for the Protection of Human Subjects of Research” better known as the Belmont Report. To ensure consistency across federal agencies, the Federal Policy for the Protection of Human Subjects, also known as the “Common Rule,” was later codified in 1991. While specific ethical requirements and procedures vary across these jurisdictional boundaries, there exists a basic set of requirements across research ethics guidelines, stemming from shared principles of respect, beneficence, and justice. These include minimizing harm, obtaining informed consent, and protecting subject privacy and confidentiality.

Minimizing Harm

Since subjects may be exposed to risks or experience harm during, or because of, a research study, a core principle of research ethics is non-maleficence—the duty to avoid, prevent, or minimize harms to subjects. Research subjects must not be subjected to unnecessary risks of harm, and their participation in research must be essential to achieving scientifically and societally important aims that cannot be realized without the participation of human subjects. Put most simply, research should not harm participants, and ethical research practices must work toward minimizing any risk of harm.
There are numerous types of harm that participants might be subjected to, including physical harm, psychological distress, social and reputational disadvantages, harm to one’s financial status, and breaches of one’s expected privacy, confidentiality, or anonymity. To minimize the risk of these harms, research ethics guidelines typically point to other key principles and operational practices, including obtaining informed consent and protecting the privacy and confidentiality of participants. These are briefly detailed below.

Informed Consent

One of the foundations of research ethics is the idea of informed consent. Simply put, informed consent means that participants are voluntarily participating in the research with full knowledge of relevant risks and benefits. Providing informed consent typically includes the researcher proactively explaining the purpose of the research, the methods used, the possible outcomes of the research, as well as associated risks or harms that the participants might face. The process involves providing the subject clear and understandable explanations of these issues, providing sufficient opportunity to consider them before granting consent, and ensuring the subject has not been coerced into participating. Importantly, obtaining informed consent requires a verification of understanding and, thus, necessitates an ongoing communicative relationship between researchers and their participants.

Obtaining consent in traditional research settings is typically done through a direct interaction between the researcher and the subject, through face-to-face mode, through telephone or video-conference scripts, or through mailed documents. The rise in Internet-based research—where researchers often interact with subjects asynchronously through online surveys or scrape data from subjects’ social networking profiles—has introduced various challenges to the traditional approach to obtaining informed consent, including verifying the identity and demographic profile of subjects, ensuring comprehension of the consent form, and obtaining appropriate documentation of the consent. Various approaches and standards have emerged in response to these new challenges to obtaining informed consent in online environments, including providing a consent form prior to completing an online survey and requiring a subject to click “I agree” to proceed to the questionnaire, embedding implicit consent to research activities within other terms of use within a particular online service or platform, or deciding (rightfully or not) that some forms of online research are exempt from the need for obtaining informed consent.

Protecting Privacy and Confidentiality

Paired with informed consent, protecting subject privacy and confidentiality is an essential component of minimizing harm in research contexts, ranging from the exposure of personal or sensitive information, the divulgence of embarrassing or illegal conduct, or the release of data otherwise protected under law. Principles of research ethics dictate that, when appropriate, researchers must take measures to protect the privacy of subjects and to maintain the confidentiality of any data collected or disseminated. Special privacy considerations are triggered when research involves the collection or monitoring of “private information,” which has a specific definition in the US federal guidelines:

“[A]ny information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information that has been provided for specific purposes by an individual and that the individual can reasonably expect will not be made public (for example, a medical record). (45 CFR 46.102[f])

This regulatory definition of “private information” has two key components. First, private information is that which subjects reasonably expect is not normally monitored or collected. Second, private information is that which subjects reasonably expect is not normally publicly available. This articulation of “private information” is also related to the concept of “personally identifiable information” (PII), which includes personal characteristics (such as birthday, place of birth, mother’s maiden name, gender, or sexual orientation), biometrics data (such as height, weight, fingerprints, DNA, or retinal scans), and unique identifiers assigned to an individual (such as a name, social security number, driver’s license number, financial account numbers, or email address).

When research potentially includes the collection of private information or PII, research ethics requires the development of protocols with sufficient safeguards to protect subject privacy and maintain confidentiality of research data. Strategies typically include minimizing the private data collected, creating a means to collect data anonymously, removing or obscuring any personal identifiers within the data as soon as reasonable, and using access restrictions and related data security methods to prevent unauthorized access and use of the research data itself.

Conceptual Gaps in Big Data Research Ethics: The Kirkegaard OkCupid Study

Most research ethics standards start from the fundamental aims of minimizing harm, obtaining informed consent, and protecting subject privacy and confidentiality, including guidelines developed specifically for researchers engaging in Internet-based research activities, such as those by the American Psychological Association (Kraut et al., 2004) and the Association of Internet Researchers (Ess & Jones, 2004; Markham & Buchanan, 2012). Yet, as Shilton (2015) notes in her study of over 200 computational researchers relying on big data-based research projects, there are “critical areas of disagreement” (p. 6) within the research community regarding
matters of consent, privacy, and related ethical dimensions of big data research. These findings confirm Moor’s (1985) prediction from three decades ago that the newness of emerging technological environments—such as big data–based research—leaves us with conceptual gaps where our earlier strategies for addressing ethical concerns fall short. Following a brief description of Kirkegaard’s OkCupid study, we expose potential conceptual gaps in how core principles of research ethics are viewed within the context of big data research, focusing on a particularly controversial case: the release of OkCupid profile data by Danish researchers in 2016.

The Kirkegaard OkCupid Study

The ethical complexities of big data research made headlines in 2016 when Danish researcher Emil Kirkegaard publicly released a data set comprising scraped data from nearly 70,000 users of the OkCupid online dating site (Kirkegaard, 2016a). Then a graduate student at Aarhus University in Denmark, collected the data set between November 2014 and March 2015 using a web scraper—an automated tool that extracts data from web pages. After creating an OkCupid profile to gain access to the site, the scraper targeted basic profile information such as username, age, gender, sexual orientation, and location while also harvesting answers to the 2,600 most popular multiple-choice questions on the site, such as users’ religious and political views, whether they take recreational drugs, whether they have been unfaithful to a spouse, or whether users like to be tied up during sex. The resulting database, along with a draft paper analyzing the data, was posted on the Open Science Framework, a web platform that encourages open source science research and collaboration, as well as to the online peer-review forums of Open Differential Psychology, an open-access online journal also run by Kirkegaard.

When asked, via Twitter, whether he attempted to anonymize the data set, Kirkegaard (2016b) replied bluntly, “No. Data is already public,” a position expanded on in the accompanying draft paper:

Some may object to the ethics of gathering and releasing this data. However, all the data found in the dataset are or were already publicly available, so releasing this dataset merely presents it in a more useful form. (Kirkegaard & Bjerrekaer, 2016, p. 2)

Kirkegaard further justified the inclusion of usernames in the released data to aid future researchers who might want to “fill in remaining [data]points” such as height, profile text, and even profile photos, which Kirkegaard’s team failed to initially capture due to technical limitations (Resnick, 2016). Based on all available documentation, Kirkegaard did not seek any form of consent—from OkCupid or its users—at any point during the collection, use, and release of the profile data, nor did he obtain any ethics approval or guidance from his institution or related oversight body.

The reaction to Kirkegaard’s OkCupid study was immediate. Numerous news outlets reported on the controversial release of the data set, and experts in research ethics were quick to point out how Kirkegaard brazenly violated a fundamental principle of obtaining consent prior to releasing sensitive or personally identifiable information about research subjects, taking issue his claim that the data were already public and free for the taking (Keyes, 2016; Markham, 2016; Zimmer, 2016a, 2016b). Aarhus University distanced itself, stating that Kirkegaard was not working on the behalf of the university, and that “his actions are entirely his own responsibility” (Resnick, 2016), and the Open Science Framework eventually removed the data set and draft paper from its website after OkCupid filed a claim under the Digital Millennium Copyright Act (DMCA). OkCupid suggested it might pursue legal action due to Kirkegaard’s violation of the site’s terms of service as well as the Computer Fraud and Abuse Act (Collier, 2016), and the Danish Data Protection Authority launched an investigation of the case, questioning the researchers’ collection, storage, and release of the OkCupid data (Cox, 2016).

While it may be tempting to dismiss Kirkegaard’s OkCupid study as the actions of a rogue and misguided researcher, this troubling case highlights numerous ways big data research presents unique ethical challenges to the research community. First, rather than discarding Kirkegaard as merely a graduate student engaged in an unofficial project, this case highlights how easy it can be to engage in big data research with personal data for thousands of subjects. Rather than needing a large research grant or computing resources— which often come with additional institutional oversight—Kirkegaard could quickly write a web scraping tool and unleash it on a social networking site to capture thousands of records virtually on his own. This reveals the ease of obtaining large data sets in today’s research environment, often outside any institutional supervision or authority. Second, Kirkegaard’s lack of formal ethical training points to a growing deficiency in how we teach research ethics to students and researchers across disciplines, and especially in the domain of big data research. Contrary to those in traditional social science fields of communication studies, sociology, or psychology, for example, many computer and data sciences are not exposed to rigorous training on research ethics. Furthermore, many jurisdictions—such as Denmark—lack a formal research ethics framework for evaluating potential research projects. As Markham (2016) notes, the emergence of big data research, like Kirkegaard’s OkCupid study, forces us, as educators, to “change the ways we talk and teach about ethics to better prepare researchers to take the extra step of reflecting on how their research choices matter in the bigger picture.” And finally, Kirkegaard’s OkCupid study helps to expose various conceptual gaps in how we approach some of the core principles of research ethics in the context of big data. Below, we highlight gaps in our conceptualizations of privacy, consent, and harm.
Privacy

The nature and understanding of privacy becomes muddled in the context of big data research, and thus, ensuring it is respected and protected in this new domain becomes challenging. For example, the determination of what constitutes “private information”—and thus triggering particular privacy concerns—becomes difficult within the context of big data research. Distinctions within the regulatory definition of “private information”—that it only applies to information which subjects reasonably expect is not normally monitored or collected and not normally publicly available—become less clearly applicable when considering the data environments and collection practices that typify big data research, such as the Kirkegaard’s wholesale scraping of OkCupid profiles. When considered through the lens of the regulatory definition of “private information,” social media postings are often considered public, especially when users take no steps to restrict access, and are thus not deserving of particular privacy consideration. For example, researchers in the Harvard “Tastes, Ties, and Time” research project (Lewis, Kaufman, Gonzalez, Wimmer, & Christakis, 2008)—where an entire cohort of college students had their Facebook profiles scraped annually for 4 years—argued that subjects do not have a reasonable expectation of privacy with their Facebook information, noting, “We have not accessed any information not otherwise available on Facebook,” and equating their collecting of the profile data with “sitting in a public square, observing individuals and taking notes on their behavior” (comment at Zimmer, 2008a). This logic mirrors Kirkegaard’s stance that “all the data found in the dataset are or were already publicly available, so releasing this dataset merely presents it in a more useful form” (Kirkegaard & Bjerreker, 2016, p. 2), and thus, there is no real privacy concern.

Yet, the social platforms frequently used for big data research purposes represent a complex environment of social interaction where users are often required to place friends, lovers, colleagues, and minor acquaintances within the same singular category of “friends,” where privacy policies and terms of service are not fully understood (Madejski, Johnson, & Bellovin, 2011), and where the technical infrastructures fail to truly support privacy projections (Bonneau & Preibusch, 2010) and regularly change with little notice (Stone, 2009; Zimmer, 2009). Similarly, numerous studies have indicated that average Internet users have incomplete understandings of how their activities are routinely tracked and the related privacy practices and policies of the sites they visit (Hoofnagle & King, 2008; Milne & Culnan, 2004; Tsai, Cranor, Acquisti, & Fong, 2006). As a result, it is difficult to understand with certainty what a user’s intention was when posting an item on a social media platform (Acquisti & Gross, 2006). It remains unclear whether Internet users truly understand if and when their online activity is regularly monitored and tracked and what kind of reasonable expectations truly exists. This uncertainty in the intent and expectations of users of social media and Internet-based platforms—often fueled by the design of the platforms themselves—creates a conceptual gap in our ability to apply the definition of “private information” to ensure subject privacy is properly addressed. As big data researchers, we must be suspect of simple justifications like “the data is already public” and critically engage with what we mean by privacy in social media data.

Consent

The conceptual gaps that exist regarding privacy and the definition of PII in the context of big data research inevitably lead to similar gaps regarding when informed consent is necessary. Researchers mining Facebook profile information or public Twitter streams, for example, typically argue that no specific consent is necessary due to the fact the information was publicly available. Yet, it remains unknown whether users truly understood the technical conditions under which they made information visible on these social media platforms or whether they foresaw their data being harvested for research purposes, rather than just appearing onscreen for fleeting glimpses by their friends and followers. In the case of the ill-fated Facebook emotional contagion experiment (Kramer, Guillory, & Hancock, 2014), the lack of obtaining consent was initially rationalized through the notion that the research appeared to have been carried out under Facebook’s extensive terms of service, whose data use policy, while more than 9,000 words long, does make passing mention to “research.” It was later revealed, however, that the data use policy in effect when the experiment was conducted never mentioned “research” at all (Hill, 2014).

In the case of Kirkegaard’s OkCupid study, it remains unclear if the user profiles harvested were publicly accessible in the first place. Kirkegaard’s draft paper reveals that initially they designed a bot to scrape profile data, but that this first method was dropped because it was “a decidedly non-random approach to find users to scrape because it selected users that were suggested to the profile the bot was using” (Kirkegaard & Bjerreker, 2016, p. 2) This implies that the researchers created an OkCupid profile from which to access the data and run the scraping bot. Since OkCupid users have the option to restrict the visibility of their profiles to logged-in users only, it is likely the researchers collected—and subsequently released—profiles that were intended to not be publicly viewable. The final methodology used to access the data is not fully explained in the article, and the question of whether the researchers respected the intentions of 70,000 people who used OkCupid remains unanswered, pointing to the complexities of ensuring informed consent existed within big data research settings.

Harm

The growing domain of big data research has also led to conceptual gaps in how we define what might be a harm,
and whether there are even truly “human subjects” deserving protection. Extending from the common arguments against any persistent privacy concerns with accessing and sharing subject information gathered from various data sources that fuel big data research—think of Kirkegaard’s simplistic claim that “Data is already public”—researchers also frequently suggest harms neither are present nor are imminently forthcoming when data are already readily available online for anyone to access and use. If a user makes their information publicly available, the argument goes, “How could there be any physical harm?”

Positions equating harm only to tangible loss or impact on a subject ignore the broader dignity-based theory of privacy harm (Bloustein, 1964). Such a stance recognizes that one does not need to be a victim of hacking or have a tangible harm take place for there to be concerns over the privacy of one’s personal information. Rather, merely having one’s personal information stripped from the intended sphere of the social networking profile and amassed into a database for external review becomes an affront to the subjects’ human dignity and their ability to control the flow of their personal information. This conceptual gap is not unique to research ethics, as international laws and regulations surrounding the collection and use of personal data similarly vary as to the definition of harm (Bennett & Raab, 2006). For example, Canadian and European Union regulations embrace a largely paternalist approach to data protection policy, aiming to preserve a fundamental human right of its citizens through preemptive governmental action, believing users must maintain control over their information to preserve dignity and autonomy. In contrast, the governance of privacy in the United States begins with the assumption that most data collection and use is both acceptable and beneficial, and limits are imposed only after some tangible harm has occurred.

Those embracing a more European approach to harm acknowledge that threats to a subject’s dignity or autonomy are as meaningful as more tangible harms, such as exposure of personal information or identity theft. But coming to this conclusion requires, at the start, the recognition that human subjects themselves are at risk within the design of big data–based research studies. In various cases, opinions differ whether human subjects are even involved in big data–based projects, providing a particularly potent conceptual gap for researchers to contend with. Much of the debate surrounding the ethics of archiving public Twitter streams centers on whether tweets are public utterances by human subjects, thus requiring ethical review, or merely the equivalent of published texts, thus exempted from any ethical concern. Similarly, researchers studying large data sets or communication network traffic, for example, frequently perceive their studies as outside the purview of ethical review boards, since, in their view, the review process is “used more in medical and psychology research at our university” (as quoted in Soghoian, 2012) or perceive review boards as bothersome barriers to achieving important research outcomes (Garfinkel, 2008).

To help address this fundamental conceptual gap, Carpenter and Dittrich (2011) introduce the notion of “human-harming research” as a variable in human subjects review in computer science and big data–based research. They worry that researchers increasingly perceive an increased “distance” between themselves and their subjects; rather than researchers engaging with subjects directly, interactions and data collection are increasingly mediated by social media profiles, data networks, and transaction logs. Thus, the perception of a human subject becomes diluted through increased technological mediation. To compensate, Carpenter and Dittrich encourage ethical review boards to transition “from an informed consent driven review to a risk analysis review that addresses potential harms stemming from research in which a researcher does not directly interact with the at-risk individuals” (p. 4) and to ultimately “transition our idea of research protection from ‘human subjects research’ to ‘human harming research’” (p. 14). In doing so, researchers who might otherwise (even if incorrectly) feel no human is directly involved in the research study would be compelled to address the ethical implications of any harm to broader populations outside the immediate research project.

**Addressing the Conceptual Gaps in Big Data Research: Contextual Integrity**

Carpenter and Dittrich’s suggestion for a reframing of research protection principles from “human subjects” to “human harming” reveals a path toward closing this particular conceptual gap. In each conceptual gap described above, avenues of reconciling the ethical dilemma and the goals of the research projects can potentially be found. To help provide a possible path for researchers, we introduce Nissenbaum’s (2004, 2010) theory of “privacy as contextual integrity” as a useful heuristic to guide ethical decision-making in big data research projects. Contextual integrity is a benchmark theory of privacy, a conceptual framework that links the protection of personal information to the norms of personal information flow within specific contexts. Rejecting the traditional dichotomy of public versus private information, the theory of contextual integrity ties adequate privacy protection to the preservation of informational norms within in specific contexts, providing a framework for evaluating the flow of personal information between agents to help identify and explain why certain patterns of information flow are acceptable in one context, but viewed as problematic in another.

Nissenbaum’s theory of contextual integrity has been applied in numerous contexts where technological developments have forced conceptualizations of privacy to be in a state of flux, including vehicle-to-vehicle communication protocols (Zimmer, 2005), search engine privacy (Zimmer, 2008b), privacy implications of cloud-based storage platforms (Grodzinsky & Tavani, 2011), smartphone applications (Wijesekera et al., 2015), and learning analytics (Rubel & Jones, 2016). Considered in the context of research ethics,
contextual integrity becomes a useful tool for avoiding the oft-repeated refrain that “the data was already public” when attempting to justify why big data research does not pose a privacy or ethical concern.

By demanding that information collection and transmission must be appropriate within a given context, contextual integrity can guide big data researchers’ attentiveness to the normative bounds of how information flows on a particular social network or community under study. Thus, maintaining the contextual integrity of those information flows can help us be attentive to many of the conceptual gaps that plague big data research ethics. To aid the application of contextual integrity, Nissenbaum provides a nine-step decision heuristic to analyze the significant points of departure created by a new process, thus determining if the new practice represents a potential violation of privacy:

1. Describe the new practice in terms of its information flows.

2. Identify the prevailing context in which the practice takes place at a familiar level of generality, which should be suitably broad such that the impacts of any nested contexts might also be considered.

3. Identify the information subjects, senders, and recipients.

4. Identify the transmission principles: the conditions under which information ought (or ought not) to be shared between parties. These might be social or regulatory constraints, such as the expectation of reciprocity when friends share news, or the obligation for someone with a duty of to report illegal activity.

5. Detail the applicable entrenched informational norms within the context, and identify any points of departure the new practice introduces.

6. Making a prima facie assessment: there may be a violation of contextual integrity if there are discrepancies in the above norms or practices, or if there are incomplete normative structures in the context to support the new practice.

7. Evaluation I: Consider the moral and political factors affected by the new practice. How might there be harms or threats to personal freedom or autonomy? Are there impacts on power structures, fairness, justice, or democracy? In some cases, the results might overwhelmingly favor accepting or rejecting the new practice, while in more controversial or difficult cases, further evaluation might be necessary.

8. Evaluation II: How does the new practice directly impinge on values, goals, and ends of the particular context? If there are harms or threats to freedom or autonomy, or fairness, justice, or democracy, what do these threats mean in relation to this context?

9. Finally, on the basis of this evaluation, a determination can be made as to whether the new process violates contextual integrity in consideration of these wider factors. (Nissenbaum, 2010, pp. 182-183)

The first six steps involve modeling the existing and new contexts, allowing a prima facie judgment to be rendered as to whether the new process significantly violates the entrenched norms of the context. These steps help us identify any immediate “red flags” that violate contextual integrity. The final steps of the heuristic involve a wider examination of the moral and political implications of the process to make a recommendation as to whether the new practice should be allowed and adopted.

The following sections apply these steps to Kirkegaard’s OkCupid study, revealing how contextual integrity’s decision heuristic might help provide clarity to the conceptual gaps plaguing in big data research ethics.

Describe Information Flows

The first step in applying contextual integrity’s decision heuristic is to identify the flows of information manifest in the context. In the context of OkCupid, there are three inherent information flows: first, a user creates an account and provides information to the OkCupid service; second, some information is made available to search engines and other non-users of the service; and third, more detailed information (such as the answers to thousands of profiling questions) are shared only with other logged-in users of the platform who happen to access another user’s profile page.

Through the course of his research and subsequent data release, Kirkegaard introduced two new information flows to the context of OkCupid: first, by creating a dummy account and running his automated script capable of accessing and archiving any user profile, Kirkegaard forced large amounts of profile data to automatically flow into his databases, and second, by releasing all information harvested by his automated script, profile data flowed outside the closed context of the universe of OkCupid users and out to the general public.

Identify the Prevailing Context

The prevailing context is the OkCupid service that facilitates logged-in users to view other user profiles to find a potential social or romantic partner, which can be summarized as an “online dating site.”

Identify Information Subjects, Senders, and Recipients

In the context of online dating sites, information subjects are the users of the site who have created accounts and provided profile information. The senders of information are users who make their profiles visible to other users. And the recipients include the dating service itself (OkCupid), other users of the service, and, to a lesser extent, the public who might have access to a limited set of profile data via search engines.

Kirkegaard’s OkCupid study expanded the scope of the general public’s role as recipients, making all profile information available to his automated script publicly accessible.
Identify the Transmission Principles

Transmission principles are the rules that govern information sharing within a particular context, and become the basis for context-specific informational norms. Transmission principles on OkCupid, like with most online dating sites, center on the sharing of personal profile information with other users on the site also looking for social or romantic relationships. While profile information can be made visible to non-users and indexed by popular search engines, users can limit visibility to only other logged-in users, thereby ensuring only other members of the dating site community have access to their profile information. Users can also limit the visibility of their “match” questions used to measure compatibility, opting to make certain responses private, and thus unseen to other users. Overall, the transmission principles assume that other (human) users will access the site to visit individual profiles and identify potential matches for social interaction.

Detail the Entrenched Information Norms

Entrenched informational norms describe the existing practices that prevail in a given context, encompassing the flows of information, transmission principles, and expectations of the actors involved. The entrenched information norms within the context of OkCupid focus on users’ ability to control the visibility of their profile information, with the expectation that only other humans who happen to visit their page will be able to access their data and that some of their data might remain invisible to all. The information norms give users control over their information flows, and selective disclosure is justified by a users’ shared desire to find social or romantic partners.

Kirkegaard’s OkCupid study appears to disrupt these informational norms by (a) creating an account for the sole purpose of harvesting all available profile data, and (b) making all profile data visible to his account publicly available. His intent was not to find a social or romantic partner, but rather to automatically collect data for research purposes.

Prima Facie Assessment

A *prima facie* assessment of Kirkegaard’s OkCupid study reveals a clear violation of contextual integrity. Kirkegaard disrupted the informational norms of the online dating context by creating a fake profile account for the sole purpose of collecting user information, using an automated web scraper to harvest the data and then releasing all the profile data to the public. He failed to obtain user consent, ignored the fact some user profile information might have been only visible due to him being logged-into the platform, and released the data into an environment beyond the expected population of recipients.

Evaluation I

Once a violation of contextual integrity is identified, we must consider the moral and political impacts to gauge the gravity of the violation. While we have no evidence of users experiencing direct harm because of Kirkegaard’s disruption of the information norms on OkCupid, users did lose their ability to maintain control of their information on the platform. Information originally shared within the contextual norms of an online dating site—where users are willing to divulge potentially private or sensitive data about themselves with others also looking for companionship—has been exposed to the public, signifying a threat to users’ personal autonomy and dignity. Kirkegaard’s actions also reveal a shift in the power structures within the context of online dating websites. Rather than being an honest member of a community of trust—where users share information with the understanding that others are doing the same, with the shared goal of seeking a partner—Kirkegaard represents an outsider who created a fake account simply to gain access to data with an automated scraping tool, without any intention of contributing to the community.

Evaluation II

The second evaluative step in contextual integrity’s decision heuristic is to consider how the new practice—in this case, Kirkegaard’s OkCupid study—might impinge on the broader values, goals, and ends of the context itself. Building on the first evaluation, where we saw potential harm to individual OkCupid members’ dignity and autonomy, as well as Kirkegaard’s presence as an imposter to the community of users, it becomes clear that the broader values of community and trust on the site were disrupted by his study. The goals of the OkCupid community—to be a trusted space to share information among members also seeking to find partners—were clearly disrupted by Kirkegaard’s actions. His presence and actions were in violation of the community principles and expectations of information flows, altering the nature of the community from one where users on equal footing share information with an understanding of mutual exchange, into a space where users might now feel concerned about their data being harvested and shared outside of the community and its informational norms.

Final Determination

Our final determination, based on the above heuristic, is that the violation of contextual integrity by Kirkegaard’s actions is not justifiable. His disruption of the informational norms within the context of OkCupid brought no benefit—directly or indirectly—to the users or the context and only degraded the values and goals of the community and its members. This conclusion is in striking contrast to Kirkegaard’s assertion that the supposed “publicness” of the data means little pause
is necessary when considering to capture and process thousands of OkCupid profiles.

**Conclusion**

For those concerned about Internet research ethics and the growing practice of publicly releasing large data sets, the rhetoric of “but the data is already public” is an all-too-familiar refrain used to gloss over complex ethical concerns, such as privacy, consent, and harm. Considering Kirkegaard’s OkCupid study, it might be easy to accept that users made certain profile information available on the online dating platform, and all the Danish researchers did was present the data “in a more useful form” (Kirkegaard & Bjerrekær, 2016, p. 2). Yet, as the above decision heuristic reveals, approaching the ethics of the OkCupid study through the lens of contextual integrity provides a very different calculus. Here, when considering the transmission principles and informational norms of the context, we can easily determine that the actions taken by Kirkegaard disrupt the contextual integrity. And once we evaluate that disruption in terms of the moral and political values of the users, as well as the broader goals of the context itself, we conclude that the impacts of the OkCupid study are not justifiable. Rather than simply waving a “but the data is already public” magic wand to make the ethical concerns disappear, walking through contextual integrity’s decision heuristic provides a much more nuanced—and contextually sensitive—approach to considering the ethics of a particular action or intervention into a research context. Embracing contextual integrity will undoubtedly guide researchers through similar ethical dilemmas in the growing domain of big data research.

The growing use of large-scale and innovative big data–based research projects and methodologies are testing the ethical frameworks and assumptions traditionally used by researchers and ethical review boards to ensure adequate protection of human subjects. The result is numerous conceptual gaps in how to apply established research ethics principles in the context of big data research. This article sought to disclose some of the ethical concerns with big data research, making transparent some of the emerging conceptual gaps. Most importantly, through the example of Kirkegaard’s controversial OkCupid study, we have shown how using a decision heuristic afforded by Nissenbaum’s theory of contextual integrity can help us, as researchers, be better positioned to understand and address the ethical dimensions of big data research projects, close the existing conceptual gaps, and thereby ensure innovative research can take place while protecting the interests of research ethics broadly.

**Declaration of Conflicting Interests**

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

**Funding**

The author(s) received no financial support for the research, authorship, and/or publication of this article.

**Note**

1. The data set remains publicly available on Kirkegaard’s Open Psych Forum, as well as on the Mega cloud storage platform.

**References**

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. Proceedings of the 6th Workshop on Privacy Enhancing Technologies, 4258, 36–58.

Barbaro, M., & Zeller, T., Jr. (2006, August 9). A face is exposed for AOL searcher no. 4417749. The New York Times, p. A1.

Bennett, C. J., & Raab, C. D. (2006). The governance of privacy: Policy instruments in global perspective. Cambridge: The MIT Press.

Bloustein, E. (1964). Privacy as an aspect of human dignity: An answer to dean Prosser. New York University Law Review, 39, 962–1007.

Bonneau, J., & Preibusch, S. (2009). The privacy jungle: On the market for data protection in social networks. In Economics of information security and privacy (pp. 121–167). Boston, MA: Springer.

Bowser, A., & Tsai, J. Y. (2015). Supporting ethical web research: A new research ethics review. In Proceedings of the 24th international conference on world wide web (pp. 151–161). Geneva, Switzerland: International World Wide Web Conferences Steering Committee.

Buchanan, E. (2010). Internet research ethics: Past, present, and future. In M. Consalvo & C. Ess (Eds.), The handbook of Internet Studies (pp. 83–108). Hoboken, NJ: John Wiley.

Buchanan, E. (2016). Ethics in digital research. In M. Nolden, G. Rebane, & M. Schreiter (Eds.), The handbook of social practices and digital everyday worlds (pp. 1–9). Berlin, Germany: Springer.

Buchanan, E., & Zimmer, M. (2016). Internet research ethics. Retrieved from http://plato.stanford.edu/entries/ethics-internet-research/

Carpenter, K., & Dittrich, D. (2011). Bridging the distance: Removing the technology buffer and seeking consistent ethical analysis in computer security research. 1st International Digital Ethics Symposium, Loyola University Chicago Center for Digital Ethics and Policy.

Collier, K. (2016, May 16). OkCupid could sue over 70k shared customer data. Retrieved from http://www.vocativ.com/318393/okcupid-leak/.

Cox, J. (2016, May 31). Danish authorities investigate OkCupid data dump. Retrieved from http://motherboard.vice.com/read/danish-authorities-investigate-okcupid-data-dump

Ess, C., & Jones, S. (2004). Ethical decision-making and Internet research: Recommendations from the AoIR ethics working committee. In E. Buchanan (Ed.), Readings in virtual research ethics: Issues and controversies (pp. 27–44). Hershey, PA: Idea Group.

Garfinkel, S. (2008). IRBs and security research: Myths, facts and mission creep. Proceedings of the 1st Conference on Usability, Psychology, and Security. Retrieved from http://static.usenix.org/event/upsec08/tech/full_papers/garfinkel/garfinkel.pdf
quest for the perfect search engine. *Journal of Business & Technology Law*, 3, 109–126.

Zimmer, M. (2009). Facebook’s privacy upgrade is a downgrade for user privacy. Retrieved from http://michaelzimmer.org/2009/12/10/facebooks-privacy-upgrade-is-a-downgrade-for-user-privacy/

Zimmer, M. (2016a, June 3). *OkCupid and the ethics of big data research*. Retrieved from http://blog.primr.org/okcupid-ethics-big-data-research/

Zimmer, M. (2016b, May 14). *OkCupid study reveals the perils of big-data science*. Retrieved from https://www.wired.com/2016/05/okcupid-study-reveals-perils-big-data-science/

Zimmer, M., & Kinder-Kurlanda, K. (Eds.). (2017). *Internet research ethics for the social age: New challenges, cases, and contexts*. New York, NY: Peter Lang.

**Author Biography**

Michael Zimmer (PhD, New York University), is an associate professor in the School of Information Studies at the University of Wisconsin–Milwaukee, where he also serves as Director of the Center for Information Policy Research. His work focuses on digital privacy, the ethical dimensions of social media and Internet technologies, and Internet research ethics.