Disconnecting the Dots: Anonymity in the Digital Age

Sydney Hanover

Governmental and corporate spying are no longer a surprising facet of everyday life in the digital age. In this paper, I expand upon the implications at stake in debates on autonomy, privacy, and anonymity, and I arrive at a definition of anonymity involving the flow between traits and the inability to connect them based on deliberate non-publication on a structurally social level. I argue that cultivating the space to remain anonymous is useful for distanced association with oneself in the purely private internal sphere, furthering a more fully examined inner association not based on a future already predicted or prematurely acted upon. The privilege of anonymity is a precondition for genuine self-relation. Later, I argue doubly against the "nothing to hide" argument, i.e., if one has nothing to hide, one has nothing to fear. Firstly, the actionability and fabrication of data make it such that it is always at risk of being interpreted as unsafe. Secondly, this argument is predicated on hiddenness as negative, which I answer with an analysis of the functionality of anonymity concerning personal growth.

I. Introduction

What we search and put on personal devices, who owns that data, and what they do with that information, is at the center of an important debate on privacy containing various opinions on what is being protected and why. This debate is not merely about words and concepts, rather, as exemplified by the extent of corporate and governmental spying in this country, all of us are affected, despite how technologically involved one may be. As I will show in this paper, at stake are the philosophical realms of autonomous deliberation, agency and personhood that underlie our actions in the digital age. These are topics that are often neglected, as we can see by the general public's blind acceptance of information banks, and even their willing participation in handing out data in forms such as social media and personalized biological information like 23andMe. Once our data is publicized, unbeknownst to us, it is not only wrung out for its future use but also may be manipulated in such a way that can affect how we relate to others—and, importantly, even to ourselves—when being anonymous is no longer a choice. As I will explain below, voyeurism in the form of unsolicited viewership can come in many forms, and often governmental and corporate spying rip away autonomy, deciding the future of personal control of information and its implications.

In this paper, I argue that the concept of anonymity, which I will define in detail below, ought to be a central focal point of the debate on privacy and autonomy, especially in the context of data-driven, algorithmic, and predictive technologies. If autonomy, the ability of an agent to act on the basis of her own authority over herself, is to be self-authored and reflective of personal deliberation in terms of growth, then anonymity ought to be protected and its centrality brought into focus. As I will show, defending anonymity as central to autonomy can elucidate key aspects of important debates about privacy.

To illustrate the centrality of anonymity in relation to privacy, I will also argue against the "nothing to hide" argument. Daniel J. Solove explains the argument as follows: government surveillance poses no threat to privacy unless unlawful activity is uncovered, in which case it should not be private—legal activity and the surveillance thereof is nothing to worry about.[1] I will refute this argument in two ways. My first strategy will be to challenge the first premise of the argument: that quotidian and legal activity can be transparent and safe. As I will explain below, movability of data, how it is disseminated and by whom allows algorithms and data banks—particularly those sustained by corporations and government—to take raw personal data and create new repossessed data sets. A repossessed data set is a data set that is taken from one data collecting entity and placed, differently categorized, into another database. The information itself is not necessarily changed, but its movement dissociates it further from where it came and its separation may shift the way that it will be used in the future. Once repossessed by the recording technology, and the industry behind it, these data sets are used for further algorithmic purposes.[2] Eventually, that individual's data does not truly belong to the agent from whom it was taken any longer. It belongs to banks of data that are stored and continuously revisited. This means that even quotidian and legal activity is not safe from how its actionability will be utilized. This is, of course, exacerbated by the fact that even if such an agent had access to such data, it would be incomprehensible to them without the algorithmic technology required to decipher its actionability.

Secondly, the nothing to hide argument does not consider how the exposition and utilization of data in the form of institutionalized surveillance policy and simpler listening devices in cell phones, for example, reflects back on personhood and growth, which will depict the implications of

[1] Daniel J. Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. Informational Privacy: Philosophical Foundations and Legal Implications)," *San Diego Law Review*, vol. 44, no. 4, 2007, pp. 745–772

[2] Following Louise Amoore, I will use the term "actionability" to refer to the way in which data becomes usable. By this I mean that traceable data like credit card purchases, flights, and numerical identifiers like social security for instance are used to glean more information about a person or her future actions. Amoore's work refers to more than the ways in which already established data points are used but how the absence of data is also acted upon. Louise Amoore, "Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times," *Theory, Culture & Society*, vol. 28, no. 6, 2011, 24–43.

a misled approach to privacy that neglects the value of anonymity. As we will see, there are some things worth keeping for oneself independently of whether or not they are things that would be considered "something to hide." In one sense, this means that this argument misses the main point of both privacy and anonymity: that we all have something to hide.[3]

The potential for invasion of personal life is ripe, as is the exposing feeling it engenders even, and perhaps especially, when it is implicit.[4] For example, unless I share information willingly, I do not want others to have access to certain traits about me, facts about how those traits are related to each other, facts about how they are related back to me, and/or, importantly, what I do with them.[5] It is this sharing transaction that, as I will show in this paper, is at the center of the flow of information I referred to above. For example, the National Security Agency, a component of the Defense Department is legally able to survey international and domestic communications under the FISA Amendment Act signed under President George W. Bush. Under this act, "foreign intelligence information," which is the primary excuse for data collection, retention, and dissemination, is defined incredibly broadly.[6] This vagueness means that Americans, their domestic and international calls, locations, and search histories are subject to government acquisition. This publicity suggests that the data of every American and foreigner, not simply those they consider "a threat" (which also has an extraordinarily broad definition), is available for legal procurement by the government.[7] What is ours, in fact, is at the disposal of the government (and corporations, which I speak less of, that are also guilty of procuring data in a manner once thought to be barred).[8] While problematic methods of collection are built into the law, practices— in terms of what they are able to collect and why—

[3] As it will become clear throughout this paper, that something should be kept from others, is independent of its moral status or social stigma. Having something to hide is not based on criminality or embarrassment but out of self-preservation, the possibility of a continued notion of self that is simultaneously changing and handling that change.

[4] Judith Jarvis Thomson inquires into the violation of rights and what that means for privacy in general by presenting several imaginary, yet very real, cases in which privacy might be being violated. See Judith Jarvis Thomson, "The Right to Privacy," *Philosophical Dimensions of Privacy*, ed. Ferdinand David Schoeman, (Cambridge University Press, 1984): 272–289, doi:10.1017/cbo9780511625138.012. I am here thinking of her example of a passerby listening to a fight she is having at home heard through open windows versus a neighbor training an amplifier to listen in (273). For most of the paper, she attempts to determine whether these two scenarios, or one or the other, violates the right to privacy and to what degree. I point this example out to note that she uses it because in both cases, intuitive discomfort is palpable and a springboard for her argument.

[5] As I will show in detail below, I do not use the term "anonymity" to refer to simple namelessness, nor do I put identity solely in that basket. Rather, as I argue, it is related to a flow of traits, behavioral propensities and embodied habits or hobbies, used to distinguish someone (not externally appropriate an identity for them).

[6] Alex Abdo and Jameel Jaffer, "How the NSA's Surveillance Procedures Threaten Americans' Privacy," *American Civil Liberties Union*, April 26, 2015, www.aclu.org/blog/national-security/secrecy/how-nsas-surveillance-procedures-threaten-americans-privacy.

[7] Abdo and Jaffer, "How the NSA's Surveillance Procedures Threaten Americans' Privacy."

[8] Adam Uzialko, "How and Why Businesses Collect Consumer Data," *Business News Daily*, August 3 2018, www.businessnewsdaily.com/10625-businesses-collecting-data.html.

also exceed lawful categories.[9]

So, why does having nothing to hide from the government still produce discomfort from the acquisition of information in the personal, and in this case technological, field? There is an underlying aspect of personhood that is extremely important to uphold and protect 一 anonymity. I would like to suggest that anonymity articulates the boundary for personal rights violation, in the form of exhibition of traits, as well as potential for human flourishing. This internal space, which anonymity seeks to protect, is perhaps to remain space—*as such*, not to be filled in—where I can connect with my most undisguised self.[10] This part of the self is to be the aspect of personhood most free from any third party intrusion, existing only for oneself.

II. Anonymity

In order to begin my analysis of anonymity it is useful to start with a working definition of the term. I define anonymity in the following way:

> The inability of any second or third party, beyond oneself, to connect the flow between traits that act as an underlying structural association of social identification that is deliberately unpublicized.[11]

As I will show later, this definition is closely related to the work of Kathleen A. Wallace, which emphasizes the sociality of anonymity, namely that everyone acts and interacts within a social context in which they can be identified, which contributes to the exhibition of their traits.[12] But first, let us take a look at each of the key terms in the definition above. By traits, I mean physical characteristics, such as hair color and height, but also habits or actions, as well as the relationships between them and their intimate, exclusive relationship to myself.

Expanding on the definition of anonymity above, consider the following example: For me to remain anonymous in one respect would mean that a second or third party observer is incapable of connecting the fact that I am graduating from the University of Oregon, my address on my license is not in Oregon, and that I am communicating with landlords in Portland. If one of these traits were taken individually, it would place me in a different geographical location along the West coast.

[9] Eric Lichtblau and James Risen, "Officials Say U.S. Wiretaps Exceeded Law," *The New York Times*, April 16, 2009, www.nytimes.com/2009/04/16/us/16nsa.html?pagewanted=1&_r=1&ref=us.

[10] I do not mean to pinpoint free will or selfhood, but to contribute a conversation on becoming attuned to being anonymous to others as well as oneself, which may be productive and weighty. Free will and the self are concepts extremely tied up in philosophy on the whole, and these topics themselves are not covered sufficiently in this thesis. Instead, my view comments on the importance of the control of one's own information, and what that might contribute to these larger concepts.

[11] The traits we display and how they integrate to form a consistency that is identifiable to one person.

[12] See Kathleen A. Wallace, "Anonymity," *Ethics and Information Technology*, vol. 1, no. 1, (1999): 21–31, doi:10.1023/a:1010066509278.

Taken together one can ascribe to a story of where I am from, where I am, and where I am going. In other words, the aggregation of spatial (location) and temporal (near graduation) traits allow a third party observer to correctly, or incorrectly, infer possible scenarios as to who I am and what I am about to be and do. It is this inference space that anonymity protects.[13] It is important to note that it is not the traits or throughlines, the connections between the connections of traits, themselves at issue in anonymity. Facts and data point to a story of someone's life. Their traits may identify them simply in some contexts, but their ability to remain anonymous refers to what is done with the information rather than what it contains. Helen Fay Nissenbaum devotes an analysis to the ways in which technology has changed in order to facilitate data aggregation and fabrication. This example is truly a euphemism for the data that is used in what she calls the "vast enterprise of meaning-making [that motivates] a great deal of collection, storage, and dissemination of information."[14] My view of anonymity is more closely related to that of Wallace, whose view addresses the "noncoordinatability of traits in a given respect."[15] Maintaining anonymity seeks to preserve a lack of comprehensive correspondence between traits. By using the term "correspondence" my framework ties anonymity to social contexts, upon which I will expand later. For now, traits identified to one person or a group must stand on the same contextual ground as the one identifying them. By "contextual ground" I mean to suggest an outline of the way in which different social networks in which people exist and act connect to one another, providing a "context" where detailed and different arenas of social life become intelligible to others. This ground does not mean to suggest a cultural or linguistic similarity, but the exhibition of traits must be able to be understood by other people. I am not considering animal behavior or extremely fringe human behavior as exhibiting the same degree of sociality, though there may be intentional interaction within these networks. To comprehend the flow of traits, they must be recognizable in comparison to others' on a social human level.

Now, let me clarify what I mean by the flow between traits. The flow between traits can be conceived of as the abstracted overarching coherence of one person's identity that allows for traits as well as throughlines to be tied together in order to denote a singular person or group. This

[13] In training predictive algorithms, the accuracy of capturing each individual instance is not really prioritized, whether it is a correct categorization of an individual or an incorrect one, the system will use it as raw data from which to learn and adapt. See Amoore, "Data Derivatives," 32-33.

[14] Helen Fay Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life,* (Stanford University Press, 2010), 45. I dedicate much of what follows to the actionability of data, but Nissenbaum also highlights an important aspect of that narrative: that inventories of information can be "effectively moved into massive aggregations and disaggregated into usable chunks … Furthermore, information begets information: as data is structured and analyzed it yields implications, consequences, and predictions" (37).

[15] Wallace, "Anonymity," 24.

perspective of materialized traits that are mapped onto an actual person does not imply a solely superimposed identity, although to remain anonymous is considered to be necessarily in relation to others. A flow is by definition not rooted or stagnant, its movement is its constancy, but the flow connects the dots between traits, and traits are always socially contextualized if they are to be recognized by others. It is important to note that anonymity, by these characterizations, is a broader term rooted in much more than safeguarding a name. The underlying structural association within these contexts is a throughline of traits that exists for the identification of a singular person. When this flow between traits is shielded, so that links cannot be made and, thus, one cannot be identified by a second or third party, one achieves anonymity.

As I briefly discussed above, in this definition I have departed from the widely accepted definition that ties anonymity to namelessness, the kind of definition that one may even find in a Merriam Webster dictionary. Being anonymous commonly refers to forms of pseudonyms or being unrecognizable. Because this paper focuses on the implications of contemporary data technologies, it is important to note, as Nissenbaum writes, that when it comes to contemporary technology "the electronic medium now offers many points of entry, some of which may be even more effective than a name."[16] Here, Nissenbaum refers to the way in which data can be inferred about a person through technology without ever knowing his or her name. Consider the following example, someone who shops at Home Depot and donates to charities that construct homes pro bono. The unnamed person can be located geographically and can be typified by her interests. This unnamed individual points out to Nissenbaum that there are other ways to gather information that are even more satisfactory than through a name. What "effectiveness" is getting at in the Nissenbaum quote above is included in the definition: relations of traits become accessible and may pinpoint a person or group. In a later section, I will explore in detail the related notion of "actionability" in this data, a concept used by Louise Amoore. These two facts about this person may be traced to her email, from which she is updated on Home Depot and her favorite charities, then targeted for advertisements on landscaping designs and manipulated into buying expensive tools, thereby making the data actionable. Capturing the electronic medium that Nissenbaum highlights requires a more thorough definition of anonymity, which will clarify my discussion on autonomy and privacy. Nissenbaum is concerned for this external identification (that of locating by another), but on which she does not elaborate. The effectiveness of the entry is what is at stake in risking anonymity and what it seeks to preserve. At stake is a zone of personhood, deliberately nonspecific and undefinable, wherein traits

[16] Helen Fay Nissenbaum, "The Meaning of Anonymity in an Information Age," *The Information Society*, vol. 15, no. 2 (1999): 141–144, doi:10.1080/019722499128592, 142.

and throughlines are melded into one another and one may grow.

Anonymity can include namelessness, but namelessness is only a portion of the larger concept of anonymity. In this paper, I will be using a version of anonymity connected to recognizable traits of identity and the flow of their linkages. At first sight, the concept of namelessness seems in fact a viable way to think of anonymity because the term denotes a certain removal of a part of identity. As mentioned above, Nissenbaum exemplifies nameless anonymity as "people strolling through a foreign city" in which "no one knows who they are."[17] There is power in this type of anonymity because being able to roam without recognition puts less anticipatory pressure, such as expecting how one will act in a foreign city setting based on already knowing their habits, on any one person. There is a lighter version of responsibility to be held. Being unrecognizable can sometimes mean having the freedom to be anyone at that given moment unbeholden to previous duties. However, even in these examples one can see that anonymity is much more complex than a name, especially in an information age sustained by electronic data gathering systems, as previously mentioned. In the first two examples about location on the West coast and shopping/donating both in relation to home repair, external agents can see what I am doing while I nevertheless remain nameless and a stranger to them. In an information age knowing people's habits and activities allows a system to at least typify me, at most use what I do for predictive purposes. Thus namelessness is only the surface of the traceability of someone, where the availability of traits and their manifestation also act as key identifiers.[18] As Nissenbaum notes, these systems can link bits and pieces of online information to a person or group without ever knowing a name, and the information they can accumulate goes much deeper than a name.[19] In the data gathering systems to which I refer, search history, online purchases, tax returns, and many more items of information are bound to one person and can reveal more about that person without ever knowing her name (this information can all be gathered from what is stored on any one computer). These items are relevant to anonymity because they are not simply pieces of information. Pieced

[17] Nissenbaum, "The Meaning of Anonymity in an Information Age," 141.

[18] Here, a proper name does indeed act as a "rigid designator," which "designates the same object in all possible worlds in which that object exists and never designates anything else." Joseph LaPorte, "Rigid Designators," *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Spring 2018, https://plato.stanford.edu/archives/spr2018/entries/rigid-designators. The object being identified when called out by name can remain that very object throughout different contexts. But, I am suggesting here, that the patterns of the flow of our traits also point to, by way of identification, to a singular person or group as well. Though the flow of traits is more malleable and subject to change than a proper name, it still acts as a rigid designator because the object remains the same, and the object remains the same within different social contexts. If that object, the anonymous person, is the same person in various social spheres, then the flow of their traits provides a more calculated rigid designator than simply her name, which likely is not needed to place traits on to a person.

[19] Nissenbaum, "The Meaning of Anonymity in an Information Age," 142.

together, they create a story (whether or not it is accurate), that are springboards from which governments, institutions, companies, and private interests target people and tell them who they are. Hence, because of the intricacy of human participation in social life, in this paper I will be using an account of anonymity tied to networks of relation that go much deeper than a name. As I will show later in detail, the insufficiency of the name is what lies in the incalculable forms of knowledge in the form of the elusive self and why the actionability of data and the gaps between data are far more important than pinning down the points of entry that negate anonymity.

Consider now that whether or not my data depicts something worth investigating or prosecuting is not up to me to decide—governments and corporations can manipulate data in general and to their advantage. Amoore cites the ontology of association as implying a relational quality between data points that becomes actionable, able to act upon.[20] The intangible link between data points is not concrete in itself, rather becomes actionable because the association and correlation between data is legitimized, even though it is an absence instead of something positive used. There is a level of abstraction based "precisely on absence, on what is not known, on the very basis of uncertainty."[21] The potential consequence is an "amalgam of disaggregated data, inferring across the gaps to derive a lively and alert new form of data derivative."[22] This associative method of interpretation can be dangerous, even if the data does not necessarily say so. For example, becoming a security risk at the airport is based on data such as checked luggage, method of payment, location leaving from and going to, and ethnicity. The associative method ties these pieces of information together to create a picture of a threatening person who is then subjected to interrogation and often racism.

Let us now return to the definition of anonymity I provided above. Social context is taken as a prerequisite to the coordinability of traits, as traits cannot stand alone within an intricate patchwork of community, notably in the technological context where platforms are interconnected by people and databases. People's traits can be thought of as their active expression—what people do characterizes parts of who they are, and when traits overlap and correlate with each other, their aggregation forms a fuller picture of who one is on the whole. Traits are not solely different patterns of behavior but how they are manifested in various and overlapping ways. For example, one person may have a hat collection, a consumer pattern, and use each style of hat for a different outdoor activity she enjoys—running, cycling, hiking, etc. These are traits in themselves and also may, for

[20] Amoore, "Data Derivatives," 27.
[21] Amoore, "Data Derivatives," 27.
[22] Amoore, "Data Derivatives," 27.

instance, suggest she is a pale person that likes spending time outside. Wallace's work highlights that people and their traits are always socially contextualized, which allows them to be placeable within a social realm at the outset.[23] Someone who is completely off the grid is not anonymous because her traits and the flow between them are not in the same sphere as others, and so they are not placeable in the language of traits agreed upon that are socially accessible. Thus, I agree with Wallace in that anonymity is not simply unknownness, in the case of being unaware of someone's existence, but rather being cognizant of someone's existence without identifying a person or group from the information available about them. Instead, anonymity shields one's identity located within a social context that would naturally allow a window into the flow of their traits that makes them not only visible but identifiable. For example, one can be visible without being identifiable. In the case of anonymous support groups like Alcoholics Anonymous, a name is stated along with the literal visibility of one's physical presence in the room, but that person is not identifiable beyond that circle. Wallace deems "network," "order," and "location" within these structures broadly as social contexts, where the examples she gives are economic, geographical, linguistic, etc. and one's position within these orders.[24] An order contains several networks of relations that overlap with other orders —for example the market and consumer networks belong to both the economic and political orders.[25] These orders make sociality more precise in examining the contemporaneousness of traits in other sectors, opening up the way in which traits, behaviors, and habits overlap in one person's life and with others'. The possibility of disclosure of identity in different sectors is extremely important to anonymity for potentially divulging choice information.[26] Divulging one's own information, or pointing out the flow of traits in order to be identified, introduces the agent as a gatekeeper for his or her own identification. This permeability folds a layer of autonomy into the function of anonymity.

Because traits in themselves, like data points, provide only so much information on a subject, topic or person, the flow between them is a more apt conception of understanding the operation of the flow between traits as opposed to description of the traits themselves. More literally I use the term flow to indicate connection. Also, I use the term "flow" to indicate changeability, in terms of growth, development, and shifting interests (for better or worse). In developing new hobbies, habits, or traits themselves, there remains a flow qua throughline that may solidify identity even through its obligatory changes (whether it shifts a little or changes completely over time). There are necessary

[23] Wallace, "Anonymity," 21-31.

[24] Wallace, "Anonymity," 25-26.

[25] Wallace, "Anonymity," 26.

[26] By "choice information" I mean to introduce the controllability of data that is at least seemingly one's own.

linkages and associations between traits but the practice of their lived embodiment for a person is constantly shifting. In this sense, I am referring to the developing to which most everyone is subject yet of which one is not necessarily aware. I am pointing to the sense of changing traits and thus how their manifestations change as a natural part of personhood. I doubt none of us are who we were, even if our hobbies and activities have remained the same. Development here is intentionally somewhat shallow and ought not to be taken positively or pejoratively; this is simply a recognition and allowance for variation in traits over time.

All this is not meant to delve into the intricate philosophical debates surrounding the nature of the soul or of personal identity, however the throughline can be said to be that which renders the same person identifiable while her traits and their manifestation change. For example, a student from Iowa that grew up on a farm may be graduating from the University of Oregon with a degree in Environmental Studies. That student previously showed her enjoyment for the outdoors by farming and producing vegetables for the farmer's market. Now, her enjoyment for the outdoors has shifted into protecting farmers through policy and she spends time talking to people in their communities, outside, but also advises local politicians on the wants of this population. She has developed, her interests have changed, but she remains herself. In the more literal (former) sense, flow signifies a more fluid interrelation between traits that may connect or disconnect with other traits of one person—a caveat that Wallace points to but does not expand upon when she says that people are a plurality of traits that are not each related to every other.[27] Thus, the flow between traits is perhaps the least material or observable aspect of anonymity, yet it is nonetheless the most definite. Traits change but a flow will remain. The space between traits is seemingly the most empty. But, I emphasize, here as well and throughout this thesis, that negativity can be productive. Traits are established and classified by their positive manifestations, how they come to be in the world, but even though the flow between traits is not positive in the sense that it impresses activities and data on the world, it is generative in the sense of creating a foundation and conditions on which occurrences happen conventionally in the world. The flow between traits is similar to how I will conceive of privacy later on as a network that is somewhat groundless but still substantially rooted and active in sensible connections between more concrete variables.

III. Privacy, Autonomy, and Anonymity

In this section I will introduce the way in which the concepts of privacy, autonomy, and anonymity fundamentally operate in concert with one another. As I will show, anonymity is a central focus in both privacy and autonomy, privacy directly pointing directly inward, and autonomy

[27] Wallace, "Anonymity," 26-27.