Privacy Myths and Mistakes:
Paradoxes, tradeoffs, and the omnipotent consumer.

Or "The no good, very bad, myths about privacy"

Kirsten Martin, PhD
University of Notre Dame
October 25, 2024

ABSTRACT:

The goal of this article is to dispel myths permeating privacy research, practice, and policy. These myths about privacy in the market – including that there is a tradeoff between functionality and privacy, that people don't care about privacy, and that people behave according to the privacy paradox – provide a distraction from holding firms accountable for the many ways they can (and do) violate privacy.

The myths emanate from outdated assumptions we make about privacy and markets, such as defining privacy as concealment and centering the consumer as the privacy arbiter. These mistaken assumptions serve to narrow industry's role and obligation to respect consumer privacy. Where privacy as concealment narrows the scope of what firms should worry about, the focus on the consumer (rather than the company) as the privacy arbiter delegates responsibility to individuals rather than firms when privacy is not respected.

However, by avoiding these mistakes and recognizing that individuals have always had legitimate privacy interests in information that is disclosed and that firms are responsible for whether and how they respect those privacy interests – I illuminate a path for future research into privacy practice and policy.

Privacy Myths and Mistakes:
Paradoxes, tradeoffs, and the omnipotent consumer.

An unfortunate mythology has developed about privacy. As more data about our lives is harvested by industry, our needs to protect that data are oddly minimized. People are framed as not caring about privacy and regularly 'giving up' privacy to go online. And, counter to endless surveys and testimony, peoples' continuing engagement with websites and apps is offered as proof that we do not care about privacy or, at minimum, we willingly trade away our privacy for the benefits of being 'online.' However, "consumers do not just say they care about privacy, but in fact often take action to protect it." (Acquisti, Brandimarte, and Loewenstein 2020, 737).

The goal of this article is to critically examine and dispel these privacy myths permeating practice, policy, and research. These myths – including that there is a tradeoff between functionality and privacy, that people don't care about privacy, and that people behave according to the privacy paradox – rely upon these outdated assumptions and provide a distraction from holding firms accountable for the many ways they can (and do) violate privacy.

Some of this confusion is from outdated assumptions we make about privacy and markets, such as defining privacy as concealment and centering the consumer as the privacy arbiter. Privacy as concealment was introduced at a time with limited computational power, when we disclosed information to trusted organizations and people one at a time. As I explain more below, privacy as concealment misses the important norms governing data that is collected by others. A second outdated assumption is where we locate the weight of responsibility to respect privacy in the market. Scholars and policy makers have increasingly looked to consumers as responsible for ensuring their privacy is respected in the market. Yet our online data market is not designed to facilitate consumers as the ultimate privacy negotiator.

However, by understanding a more descriptively valid, normatively guiding, and empirically supported definition of privacy, I offer important implications to policy and paths for privacy research. Previous assumptions about privacy may have worked when economists were first thinking about privacy in the 1960s – but not today.

1. UPDATING OUR ASSUMPTIONS ABOUT PRIVACY

1.1 Outdated Assumption 1: Defining Privacy as Concealment.

Privacy discussions focus on *justifying* why privacy is important (Bloustein 1964; Regan 2011), or *identifying harms and values* at stake with privacy (Citron and Solove 2022; Cofone and Robertson 2017; Calo 2011), and *protecting* privacy (Hartzog 2011; Brunton and Nissenbaum 2011). But as an initial assumption, privacy discussions must begin with an understanding of what privacy is before we decide how to measure it, justify it, or defend it. And it is at this base assumption where I argue many have made a mistake.

Defining privacy as concealment relates privacy to the degree we are accessible to others: we have privacy when we are concealed, and we do not have privacy when we are seen by others or our information is disclosed. This approach to consumer privacy has been popular in philosophy (Gavison 1980; Nagel 1998; DeCew 1986), law (Gavison 1980) and, most importantly for today, economics (Stigler 1980; Posner 1981). As noted by economist Alessandro Acquisti, privacy as concealment has been adopted widely within the study of privacy, firms, and markets (Acquisti, John, and Loewenstein 2013, 251; Acquisti 2023).

This definition has been attractive to researchers since privacy-as-concealment is easy to identify and model in empirical work: people make a binary (and easily measured) decision to either conceal information (i.e., protect privacy) or disclose it (i.e., relinquish privacy) (Martin 2022, 494). For example, research measuring factors influencing disclosure can then be framed as factors influencing consumers giving up privacy (Hallam and Zanella 2017) and whether someone discloses information is then a measure of whether they care about privacy (Beresford, Kübler, and Preibusch 2012). For industry, defining privacy as concealment means people 'give up' privacy when using a website or app, and these firms then have no privacy obligations about data they have gathered. Firms are then (mistakenly) permitted to gather, aggregate, sell, and use the information without any privacy interest at stake (Martin 2022).
For example, when people use website, the individuals are giving up their privacy interest in how that data is shared or used (according to privacy as concealment). This would mean that consumers merely engaging with apps or websites have no interest if an ad exchange shares their location and web history with data traffickers on the exchange.[1]

[1] https://storage.courtlistener.com/recap/gov.uscourts.cand.375820/gov.uscourts.cand.375820.690.0_1.pdf

However, defining privacy as only that which is concealed misses our experience living our lives in pubic while having privacy respected (Strandburg 2010; Nissenbaum 1998; 1997; Cohen 2012). While defining privacy as concealment protects hidden or concealed information where "people may escape the prying and interference of others," such an account is incomplete by ignoring the protection that is needed with people and information that is shared, collected, or revealed (Nissenbaum 1998, 207). Most of our lives are conducted in 'public' and with others, yet this minimal, thin definition of privacy stops providing guidance once individuals step out into public, engage with someone else, go online, use their phone, etc (Strandburg 2010).

In fact, our oldest stories about privacy center on privacy when out in 'public.' The seminal privacy article by Warren and Brandeis is known to have emanated from a need for privacy being respected at a wedding (Warren and Brandeis 1890). But an even older tale is the 11th century story of Tom the Tailor ('peeping tom') looking at Lady Godiva when he was not supposed to while she was riding a horse in a *public square* (Davidson 1969). We have always had a need for privacy in 'public' or when we are exposed.

To be sure, the designers of this minimal approach to privacy did not envision the data markets of today, where data traffickers (Scholz 2019) are able to buy and sell consumer data without interacting with the subject of the data (Shilton et al. 2021). Originally, firms were assumed to never gather too much information due to the assumed cost to collect and store that information (Posner 1981; Stigler 1980). We could assume 60 years ago that firms would always seek information directly from the consumer for immediate use, and extraneous information was costly and would be ignored (Martin 2022; Stigler 1961).

This brings us to the first way privacy as concealment fails us: *privacy as concealment is not descriptively valid,* since individuals have throughout time retained expectations as to how information is gathered, shared, and used even when the individual or data is 'in public' and revealed. And empirical research only reaffirms the nuanced but clear norms about how privacy is expected with data that has been collected and with people who are not concealed.[2]

[2] For example, we retain expectations of privacy about our emotions (Roemmich and Andalibi 2021), information in public databases (Take et al. 2022), location (Martin and Nissenbaum 2020; Acquisti and Gross 2006), in our moods (Zhang et al. 2021). Even with videos of us in public, we care about the purpose for which footage is captured and analyzed, the particular venue where it is captured, and whom it is shared with (Zhang et al. 2021).

And, we have privacy needs and interests in regards to the data that is collected about us for good reason: because we can be harmed by the use of that data (Citron and Solove 2022; Citron 2018; Cofone and Robertson 2017; Calo 2011), the data may render us uniquely vulnerable (McDonald and Forte 2020), we may be manipulated by the use of that knowledge (Martin 2022; Susser, Roessler, and Nissenbaum 2019), and new knowledge can be created about us given each piece of 'public' data – knowledge that we did not want to be shared (Schoenebeck et al. 2024).

However, equally important, defining privacy as concealment is *also not normatively desirable*. Privacy is a desirable goal or value as well as being instrumental to other goals such as human flourishing. Privacy is important to individuals and society similar to love, trust, security, etc. For example, trust is a good thing that is a worthy goal to achieve for individuals, relationships, and society. Seeking to achieve trust is normatively desirable and violations of trust are not desirable. Privacy is similarly positioned as normatively desirable – good for individuals and society (Cohen 2012; Richards 2015).

Privacy, when defined as only achieved when you are fully concealed, positions privacy as a state of solitary inaccessibility – which is actually undesirable (Martin 2016b). A state of inaccessibility is not sustainable since people need to have relationships and coordinate activities so survive (Dennett 1995; De Waal and De Waal 1997). Individuals need to share information – including intimate information – as a form of social self-authorship (Susser 2016) and to engage in self-expression (Citron 2022). Protecting information shared within a trusting relationship allows people to speak freely, experiment with ideas and identities, develop agency, and create relationships (Citron 2022; Waldman 2018; Hildebrandt 2019). Respecting privacy with disclosed information is also important to converse and trade (Singleton) and for a flourishing democracy (Reidenberg 2014; Regan 1995; Richards 2015).

By limiting privacy to only that which is hidden or inaccessible to others, privacy as concealment not only misses the privacy we need with shared data, but also posits privacy as something that is undesirable and a form of punishment. Our need to share information and form relationships is so strong and integral to being human that a state of perfect inaccessibility—or a completely solitary existence where a person and their information is kept inaccessible from others—is considered an extreme form of punishment (Tufekci 2008). Defining privacy as concealment is neither practical nor desirable and, ironically, renders privacy as a form of punishment (Martin 2016b, 556).

1.2 Updated Approach: Privacy respecting data norms.

As noted by prominent economists, the study of consumer privacy within markets must move past relying upon these definitions that do not require privacy to be 'given up' upon disclosure (Acquisti 2023). And privacy definitions exist that support the sharing and collection of data within norms of privacy. For example, rather than privacy as concealment, more context-dependent definitions of privacy posit that an individual who shares information does so within a community, relationship of trust, or within a particular context (Hartzog 2011; Richards and Hartzog 2020; Waldman 2018; Nissenbaum 2010). Specifically, people engage with an organization or person for a specific purpose or goal, and privacy is respected when the norms of appropriate flow for that context are respected (Nissenbaum 2010). That context, e.g., healthcare, education, banking, etc, then drives what information should be collected, how that information should be collected, who can have access to that information, and how that information should be used (purpose or goal) (Martin and Nissenbaum 2015). Importantly, people have privacy interests in how data is used, stored, and shared with information that is disclosed or collected. These organizations that collect our data then have duties and obligations to protect our information within those privacy norms (Richards and Hartzog 2021; Lobschat et al. 2021).

And empirical research supports these approaches showing that people have nuanced privacy interests in information that is disclosed, that how firms use data that is collected is relevant to whether the firm meets the privacy expectations of individuals, and that individuals approve of their data being used to benefit themselves and others while disapproving of the use of the same data for manipulation or marketing (Martin, Nissenbaum, and Shmatikov 2024).

For example, when engaging with an app, users find the collection and sale of their location data to data brokers to be a privacy violation (Martin and Nissenbaum 2020; Martin, Nissenbaum, and Shmatikov 2024).

1.3 Mistake #2: Placing Weight of Privacy Responsibility on Consumer.

The second mistaken assumption is in focusing the weight of responsibility for ensuring that privacy is respected on the consumer. The current narrative about privacy online centers a (hypothetical) well-informed and empowered consumer. U.S. regulations, policies, and research posit the consumer as needing to make privacy choices with adequate notification. (Chander, Kaminski, and McGeveran 2020; Richards and Hartzog 2018). As Solove summarizes, "Unfortunately, existing privacy regulation relies too heavily on privacy self-management as a

means of privacy protection" (Solove 2021). This mythical consumer, who has existed in historical fantasy narratives of past industries (e.g., auto safety, tobacco), is expected to counter the increasing onslaught of data collection techniques and volume of data traffickers as well as the associated novel privacy vulnerabilities as they navigate websites, apps, or even just drive around.[3]

And research has centered the individual, rather than industry or firms, as making privacy calculations in using an app or website. The privacy calculus view of consumer decisions posits that consumer privacy choices are driven by a systematic weighing of the benefits of information disclosures against the perceived privacy risks from such disclosures (Milne and Gordon, 1993; Dinev and Hart, 2006). For Westin (2000), consumers are shrewd privacy balancers who weigh the value to them and society of various business and government programs calling for personal information. (Adjerid, Peer, and Acquisti 2018). And when privacy is not respected, e.g., when information is in the wrong hands or used for the wrong purpose, the privacy calculus model is used to understand how people weigh the benefits and risks disclosing information rather than question why firms collect information or how firms make decisions to collect, use, share, consumer information, (e.g. Jung and Heo 2022; Segijn and Voorveld 2021; Youn and Shin 2020; Zarouali et al. 2019). (Boerman and Smit 2023) (Milne and Gordon, 1993; Dinev and Hart, 2006).

Placing the onus on consumers to correctly navigate data practices (and ensure their privacy needs, preferences, and expectations are realized) benefits firms with whom the consumers are 'negotiating.' Since the focus of researchers, policy makers, and courts is on consumers' choice, rather than the practices of the firms, firms have an incentive for their notices to be opaque (Obar and Oeldorf-Hirsch 2020; Chen et al. 2024) and even deceptive (Sivan-Sevilla, Nissenbaum, and Parham 2022) and provide choices layered behind pages of instructions or no choices at all (Waldman 2020; Gunawan et al. 2024).

1.4 Issues with this approach

A focus on the consumer as empowered negotiator works for only specific market situations. For example, in a market with low information asymmetries, minimal uncertainty, and where friction (transaction costs) between market choices is minimal, a consumer's choice should closely align with their needs, preferences,

[3] This mythical consumer, all knowing and powerful, is also the worst negotiator in the history of markets. Not only are their privacy needs not realized in the practices of firms but their data is then used to harm them (Bhargava and Velasquez 2021) or at least lower consumer welfare (Schnadower Mustri, Adjerid, and Acquisti 2023).

and expectations. A large farmer's market is a classic example of such a market as well as some online markets with adequate safeguards in place to communicate quality and provide enforcement mechanisms.

In today's data markets, to achieve an all-knowing, empowered consumer, consumer data flows would need to be known and privacy choices between competitors would be apparent and frictionless. Violations of privacy would be easily identified and quickly remedied to ensure the market functions and consumer choice is paramount. Key for such a market is (a) critical attributes of the product or services (data flows) are known at the point of a decision, (b) choices between goods and services are easy with few transaction costs to the consumer, and (c) market corrections are felt by the firms that violate the preferences of the consumer to ensure that consumer choice is meaningful.

This consumer-empowered market is the market economists envisioned when putting forth privacy as concealment as a theory with a focus on the consumer as bearing the weight of ensuring their privacy preferences, needs, expectations are met. The economists presumed that information would only be shared if consumers trusted the other party (and that party would be known) and that information sharing would always be beneficial to the consumer (Posner 1981; n.d.; Stigler 1980). If the collection, sharing, and use of data violated privacy, the resultant cost of upsetting individuals was assumed to be felt by those firms actually gathering and storing the data. Therefore, all collection, sharing, and use of information would be sanctioned by the empowered consumer (Martin 2022, 497–98).

We have assumed a data market similar to fast food fries. The quality of the fries is apparent to the consumer, choices between restaurants are easy. If we don't like fries, we can return them. We also can never go back to that particular restaurant again.[4] We can identify not only with whom we are transacting but also the terms of the transaction, quality of the goods, etc.

However, information about privacy is not known by consumers; firms create a situation with high information asymmetry and uncertainty. In fact, a study showed that when researchers provided specific information about what data would be collected and how that data would be used and shared, consumers *did* make better choices that aligned with their privacy needs (Tsai et al. 2011). Yet, in todays' actual market, notices are obscure and even deceptive (Sivan-Sevilla, Nissenbaum, and Parham 2022; Obar and Oeldorf-Hirsch 2020). Choices are hidden and defaults are

[4] It should be noted that the market for fries is also heavily regulated with minimum safety standards. No such minimum standards exist for privacy in the U.S.

set to favor the firm rather than meet the privacy needs of the consumer (Gunawan et al. 2024). There is not a remedy when privacy is violated, such as if information is sold to a data trafficker or used in a manner that violates privacy. In such an obscured, uncertain market situation, relying on consumer choice as an indicator of their preferences, needs, and expectations creates consumer risk and is actually a breeding ground for exploitation where firms can take advantage of consumers with little knowledge and even less power.[5]

Worse still in our current situation, consumers do not know they are in a transaction with another party. For example, a reader of the Washington Post does not know that they are in a transaction with trackers and ad exchanges. Yet, the choice to continue to read a website is used as an indicator that individuals have consented to an ad exchange collecting, using and even selling their data by industry.[6]

A fundamental assumption in a consumer focused market, based usually on transaction cost economics, is that we know and can identify the other party to a transaction.[7] In our data markets, not only do we have information asymmetries as to the price and quality of the 'exchange' but we do not know the actors with whom we are supposedly transacting. On a given website or app, we are not shown the trackers or ad exchanges, who are collecting our location, search terms, and browsing history yet are framed as responsible for the collection and sale of data about us.

Consider the similarity to how the economist Alessandro Acquisti explains the current issue with privacy in today's market:

> As we travel on a crowded train, we quickly sense another person's peeking at the documents open on our screen; as we walk in a street, we notice the steps of someone following us too closely. On the Internet, *we do not see or hear Facebook or Google*

[5] When parties are vulnerable in the exchange, reputation (Akerlof, 1970), trust (Kollock, 1994), and credible contracting (Williamson, 2002, 2005) become critical. In fact, trust is more needed in situations where information asymmetries introduce significant risks (Kollock, 1994). As noted by kollock, "risk creates a breeding ground not only for trust but for exploitation as well" Kollock, 1994, p. 320. (Martin 2013)

[6] https://storage.courtlistener.com/recap/gov.uscourts.cand.375820/gov.uscourts.cand.375820.690.0_1.pdf

[7] A classic scholar for transaction cost economics is Coase – and his more famous example had a rancher and farmer with properties next to each other. Coase showed how the two parties could negotiate property rights, depending on transaction costs, when the rancher's animals damaged the farmer's crops. However, parties to the transaction were neighbors and easy to identify. Similarly, Coase's example of a train creating sparks assumed that the community through which the train traveled could identify the train. Currently we have a market where the market actor, who is collecting, using, and selling data about us thereby violating our privacy, is not identified to the user and neither is the collection, use, and selling of data about us. Our current approach to privacy online would be as if the farmers crops were damaged but not knowing who the perpetrator was – but then blaming the farmer for his crops being damaged because he did not negotiate well enough.

> *tracking us across all sorts of digital domains*. Notice and consent mechanisms—as well as educational or informational interventions—fail because they do not account for the underlying nature of consumer privacy decision-making (Acquisti 2023, *italics added*)

Acquisti refers to this onus on the consumer to be the arbiter of privacy online as "consumer responsibilization" which he defines as "asking consumers to take charge of a problem they did not create and cannot really control" (Acquisti 2023). And increasingly scholars have called for greater responsibility to be shifted to firms as in terms of privacy and data governance (Lobschat et al. 2021; Martin 2016a).

The assumed empowered consumer has become an embattled consumer taking on the responsibility of an industry whose hidden tactics are difficult to reign in even for regulators. In fact, firms have taken to deceptive design and notices to trick users into disclosing data and consumers are then expected to go to extraordinary lengths, including downloading additional software, to combat industry's attempts to violate privacy.[8] Centering the consumer as responsible for ensuring privacy is respected online does not fit our current online data markets.

1.5 Limited Scope of Corporate Responsibility

These outdated assumptions – defining privacy as concealment and centering the consumer as the privacy arbiter – combine to minimize the role and responsibility of firms in respecting privacy in our current environment. Defining privacy as concealment narrows the scope of responsibility since firms would have no responsibility to protect information post-disclosure. And placing the weight of this privacy decision on the consumer means the website or app has a limited role in ensuring this privacy decision is made 'correctly' since the consumer is held responsible for their market 'choice.'

These two assumptions may have worked at a time with different market structures and different technological abilities. However, the ability to collect, sell, and use data within a hidden data market and with so much of our lives online, mediated by these technologies, means that assuming privacy is only that which is concealed and focusing on consumers as empowered arbiters of privacy has outlived societal

[8] This focus on the consumer as responsible has become so normalized that consumers are now expected to develop and employ effective counter measures against market actors.. Researchers operationalize the value placed on enacting privacy as whether or not consumers take extraordinary actions in their battle with data traffickers (e.g., downloading and using anti-tracking devices, using VPNs, installing obscuring technology, providing fake information, etc). Most industries are not in such a combative stance with their key stakeholders.

advances. However, as we focus on next, these assumptions have infected pervasive privacy myths that flow throughout public policy, practice, and research, including the tradeoff between privacy and functionality, the unconcerned consumer, and the privacy paradox.

2. PRIVACY MYTHS

2.1 Myth #1: The tradeoff between privacy and functionality (innovation, efficiency, etc).

The first myth told about privacy is that there is a tradeoff between privacy and functionality (efficiency, innovation, etc). In research, this privacy tradeoff is operationalized as whether an individual will disclose information for beneficial uses (Jiang et al., 2013; Xu et al., 2011; Dinev & Hart, 2006). This tradeoff myth assumes people sharing information for functionality (innovation, personalization, recommendations) is framed as people trading privacy for functionality. For example, data sharing is framed as an exchange of privacy interests for personalizing services (Xu et al. 2009; Kim et al. 2019), locating someone on a map, or recommending products (Xu, Luo, et al. 2011) (Al-Jabri, Eid, and Abed 2019). If privacy interests are only for data that is concealed, maintaining privacy requires withholding information from others would mean decreased functionality (Calo 2015, 653).

Perhaps more importantly, the tradeoff myth continues in the larger study of public policy and market governance. In general, sharing information is helpful for efficient transactions, enhanced functionality, and product innovation (Acquisti, Taylor, and Wagman 2016; Hayek 1945; R. Calo 2015). This approach to defining privacy-as-concealment renders privacy inefficient to a functioning market since (in principle) relevant, concealed information could be helpful to better transactions (Stigler 1961; Posner 1981). Economists could then summarize: "Privacy is harmful to efficiency because it stops information flows that would otherwise lead to improved levels of economic exchange" (Hermalin and Katz 2006, 211).

Within public policy, we see this myth when privacy regulations are posited as undermining innovation, produce improvements, advancements, etc. For example,

> This hearing will undoubted include questions about balancing the tradeoffs between privacy and the ability to share our lives, make our voices heard, and build online communities through social media. It makes little sense for Congress to impose a one-size-fits-all answer to these questions, given that individuals value the tradeoffs very differently. Addressing data

> privacy through competition, on the other hand, allows consumers to answer these questions for themselves according to their individual values. [9]

Richard Murphy (Murphy 2017) summarizes the tradeoff argument, "the consensus of the law and economics literature is this: more information is better, and restrictions on the flow of information in the name of privacy are generally not social wealth maximizing, because they inhibit decision-making, increase transactions costs, and encourage fraud."[10] By (incorrectly) equating privacy as only respected when information is concealed, respecting privacy is equal to inefficiency, loss of functionality, etc.

We also see this type of 'forced' tradeoff with public policy recommendations by anti-regulation (or self-governance) advocates. For example, in congressional testimony self governance is needed due to

> "the inevitable trade-offs… between privacy and other values--such as: …innovative media and services …. diversity and competitiveness of an Internet ecosystem …ease of use for consumers … innovation …and so on."[11]

Similar to the hypothetical navigation app, this grand tradeoff claims users can either allow the exploitation of consumer data by data traffickers or have no Internet at all. However, this ignores the many options that do not hold consumer privacy hostage such as showing ads that are not based on privacy-violating data or developing an ad exchange that does not sell consumer data to third party data traffickers as a core part of the business. It is possible to have functionality and the Internet and even ads without violating privacy of users.

Privacy is a tradeoff if and only if one (mistakenly) defines privacy as concealment. For the case of ad exchanges that sell user data, including search terms, location, web history, identification, etc, to data traffickers when attempting to find an advertiser for a site, the tradeoff argument would e that people benefit from engaging with websites and typing in search terms into a search engine or looking at a website means that people trade away their privacy by providing that data.

However, a firm could *design* a tradeoff whereby users are forced to have their privacy violated if they want a functional product or service. Importantly, a privacy

[9] https://www.congress.gov/event/115th-congress/senate-event/lc64510/text?q=%7b%22search%22%3a%22privacy+%5c%22trade-off%5c%22%22%7d&s=7&r=3

[10] Calo summarizes: e.g. of the argument: "firms will not be able to generate new, useful content or services without the largely unfettered ability to collect, process, and disseminate information. " (r. Calo 2015, 656) but firms have made this argument about labor, raw materials, ability to pollute, etc. And we do not take them seriously when they claim the need for 'unfettered' access in order to make their jobs easier.

[11] https://www.congress.gov/event/112th-congress/senate-event/lc2556/text?q=%7b%22search%22%3a%22privacy+%5c%22trade-off%5c%22%22%7d&s=7&r=2

'tradeoff' is not necessary – firms can (and should!) collect data to improve services while respecting privacy. For example, sharing location data in order to use a navigation app is sharing appropriate data for the context (navigation) and the use is limited to the purpose of the context. The app could offer a service where they collect location data only for navigation purposes which would respect the contextual privacy expectations of users – no tradeoff required. However, if the navigation app forced users who shared their location data into an ad exchange whereby the location data provided for navigation was also sold to data aggregators on the ad exchange, the navigation app would have *designed* a tradeoff that was not required. The design decision to give users the 'choice' to either not share location data or share location data and allow the app to collect and use location data for both navigation as well a behaviorally targeted ads (and sell the data to data brokers in the process) forces the user to not have their privacy expectations respected in order for the navigation app to work. But this is a design choice by the app and not required.

Table 1: Tradeoff Myth Assumptions and Alternatives.

Tradeoff Myth	Mistaken Approach	Change: Stop equating privacy with concealment	Alternative Approach
Research	When subjects share information or engage online, we can assume they gave up their privacy and traded privacy for functionality.	Privacy is respected when the norms of appropriate flow are respected within the context: what information is collected and how, who receives the information, how the information is used.	Research on the benefits of sharing information still applicable to questions of information disclosure without having to equate information disclosure with giving up privacy.
Practice	Consumers give up privacy when they decide to go online		Using data for functionality is within privacy norms. Users have privacy expectations post disclosure.
Policy	Any laws restricting the flow of information undermines innovation, efficiency, and functionality.		Laws limiting the use, collection, sharing, and storage of information to within the context in which it is collected respects privacy and allows for functionality, efficiency, and innovation.

Designed privacy 'tradeoffs,' whereby functionality is held hostage until the user agrees to privacy violating practices of a firm, is usually not possible in a competitive market with low information asymmetries. Consumers would simply go to a competitor that offers functionality without privacy violations. However, given the second common mistake, we also tend to blame the consumer rather than question the structure of the industry or design of the business model (or both) when we see privacy violating behavior.

2.2 Myth #2: People don't care about privacy.

A second myth that permeates research and public policy is that people do not care about privacy. More specifically, while a few fundamentalists care about privacy, many people are unconcerned about privacy or are privacy pragmatists (Urban and Hoofnagle 2014). And because of this supposed heterogeneity in privacy concerns, users should be able to choose whether or how privacy is respected in the market. As summarized by Acquisti et al "Contrary to depictions of online sharing behaviors as careless, we show how consumers fundamentally care about online privacy, and present evidence of numerous actions they take to protect it" (Acquisti, Brandimarte, and Loewenstein 2020, 736)

Yet the myth of the consumer unconcerned about privacy prevails. The myth originated from a specific survey on privacy concerns devised by Alan Westin. Westin's privacy concern measurement from 1991 places respondents into groups he labeled privacy fundamentalist, privacy pragmatist, or privacy unconcerned based on their responses to three questions (Westin 1991). These labels are then used to justify that people have heterogenous concerns about privacy, including those 'unconcerned' about privacy. However, the survey prompts used to create these groupings are broad and worth revisiting considering how prevalent privacy concern measurements are in policy and research.

In the original case of Westin's categories in 1991, respondents were asked whether they agreed or disagreed with three prompts in Table 2.

Table 2: Prompts for Westin's privacy concern measurement

Prompt	Fundamentalist (if all 3 match)	Pragmatist	Unconcerned (if all three match)
1. Consumers have lost all control over how personal information is collected and used by companies.	Agree/Strongly Agree	Everyone Else	Disagree/Strongly Disagree
2. Most businesses handle the personal information they collect about consumers in a proper and confidential way.	Disagree/Strongly Disagree		Disagree/Strongly Disagree
3. Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today	Disagree/Strongly Disagree		Agree/Strongly Agree

In Table 2, a person labeled a "privacy fundamentalist" would need to (a) agree that consumers lost all control of data and (b) disagree that most businesses protect data and (c) disagree that existing privacy laws and organization practices protect privacy (Martin and Nissenbaum 2015). Few privacy fundamentalists exist. Privacy pragmatist is the most common label: someone would only need to choose 'neither agree or disagree' with one of the three statements to be labeled a privacy pragmatist.

The use of privacy concern labels is attractive for industry because if there is variance in how much people 'care' about privacy, i.e. heterogeneity in consumer

preferences, the market is assumed to be the most efficient mechanism to allow these consumers to find their privacy preferences.

Along these lines, Westin believed that people wanted to determine for themselves how information is communicated to others.[12] Westin testified that replying "neither agree or disagree" to one of the prompts (and being labeled a privacy pragmatist) meant respondents favored "voluntary standards and consumer choice over legislation and government enforcement" (Hoofnagle and Urban 2014, 268) – even though respondents were never asked about regulation. Expert witnesses now cite Westin's finding that people vary in how they answer these privacy concern questions to argue that privacy laws will get in the way of not only innovation but the ability of unconcerned consumers to transact.[13] Building on the idea that people vary in the 'concern' for privacy, privacy scholars went on to build survey instruments focused on measuring a 'concern for privacy' that are cited and used thousands of times (Smith, Milberg, and Burke 1996; Dinev and Hart 2006; Xu, Dinev, et al. 2011; Malhotra, Kim, and Agarwal 2004)

The variance as to how people answer general questions about privacy should not be surprising. Questions about a general attitude, disposition, or belief *should* elicit a range of responses. As noted by Schaeffer and Presser, in the aptly named "The Science of Asking Questions" (Schaeffer and Presser 2003), survey questions about a general phenomenon such as 'concern for privacy' can be ambiguous in two dimensions: in the object as well as in the evaluative dimension of the prompt. For example, "a respondent might be asked to express approval or disapproval (evaluative dimension) of the Agricultural Trade Act (object), or to rate himself (object) on happiness (evaluative dimension)" (Schaeffer and Presser 2003). For privacy concern survey instruments, the respondent must wrestle with both types of ambiguity – the concern (evaluative dimension) about privacy (object).

First, privacy concern is an ambiguous term because the concept of privacy – the object of the question -- depends on the context of the transaction, what information is collected, how that information is collected, shared, used, etc. So asking questions about "privacy" or even about a particular type of information does not

[12] "e.g. "An important conclusion flows from the observation that privacy is subjective: government regulation in the name of privacy can be based only on guesses about what ``privacy'' should look like." https://www.congress.gov/event/111th-congress/senate-event/LC5538/text?q=%7B%22search%22%3A%22%5C%22Westin%5C%22+privacy%22%7D&s=9&r=20

[13] https://www.congress.gov/event/116th-congress/senate-event/LC67183/text?q=%7B%22search%22%3A%22%5C%22Westin%5C%22+privacy%22%7D&s=9&r=8

provide the respondent with the necessary information to evaluate the object of privacy. Judging the privacy of location data, for example, requires the respondents to have a common understanding of how location information is collected, used, stored, and shared and by whom and within what context. This would be similar to asking a general 'security' concern question or a general 'trust' question (which we do!). There will be variance because individuals are able to project their assumptions onto the question. When we ask about privacy concerns, someone could assume we mean government collection of data or only about medical data or only about criminal cases, etc. This is also true of many of our privacy constructs.[14]

In fact, research has found that clarifying the object of concern (e.g., privacy or privacy laws) in Westin's studies changes respondents' answers. Chris Hoofnagle and Jennifer Urban show that people who Westin categorized as privacy "unconcerned" or privacy "pragmatist" tended to falsely believe that protections were in place and were more ignorant of actual privacy rules, regulations, and practice than people Westin categorized as privacy "fundamentalists." When informed of the what data flows were possible as well as what legal protections existed, privacy pragmatists made decisions more consonant with privacy fundamentalists (Hoofnagle and Urban 2014). Variance in Westin's privacy concerns is partially due to the ambiguity in the object of concern.[15]

The second area of ambiguity is the term 'concern' – the evaluative dimension -- in Westin's (and similar) survey questions. Asking respondents if they are *concerned* about X captures (a) if they <u>care</u> about X, and (b) <u>the likelihood</u> that X could happen. For example, if I were to ask respondents about their concern as to failing seatbelts, assuming we get past a common understanding of the object of the failing seatbelts, we would get very low concerns because (a) while we care about what

[14] "Our analysis reveals considerable misalignment between the constructs associated with the statements and participant understanding. Many statements used in scales or that we devel- oped with the intention to measure constructs such as privacy concern, are seen by survey participants as describing other constructs, such as privacy preferences" (Colnago et al. 2022).

[15] Westin's categories are capturing a knowledge gap as to the company policies and existing regulations as to privacy online, i.e., People who were labeled privacy fundamentalists by Westin's categories were more knowledgeable about practices and protections that exist. In fact, more recent conceptualizations of privacy concerns include items such as "I am concerned that the information I submit to this website could be misused," Heng xu et al., "information privacy concerns: linking individual perceptions with institutional privacy assurances," *journal of the association for information systems* 12, no. 12 (2011): 1table b.1 (four prompts to measure privacy concern : "1. I am concerned that the information i submit to this website could be misused. 2. I am concerned that others can find private information about me from this website. 3. I am concerned about providing personal information to this website, because of what others might do with it. 4. I am concerned about providing personal information to this website, because it could be used in a way i did not foresee.").

could happen (we don't want to get hurt!), (b) we don't think that will ever happen because we trust automobile makers now (and the NTSB…). Low concern evaluations can come from caring a great deal but believing the likelihood is very small – or low concern evaluations in general can come from not caring. For privacy, low concern for privacy could mean that respondents would care a great deal but do not believe a privacy violation would happen in that they trust online firms.

Table 3: Unconcerned Consumer Myth Assumptions and Alternatives

Unconcerned Consumer Myth	Current approach	Change: Stop blaming consumer	Alternative Approach
Research	Westin's survey questions show people differ in how concerned they are about privacy and decisions about privacy should be left to consumers.	Variance in how people answer Westin's questions is a measurement of the ambiguity of Westin's questions.	Westin's survey questions measure trust in business generally (therefore not concerned) and a lack of knowledge about data flows. Measuring privacy preferences and needs should be done based on specific contexts.
Practice	Organization should default to less privacy protective policies since consumers differ in how much they care about privacy and many do not care.		Measuring user privacy needs should be done within the specific context.
Policy	Heterogeneity in how much people answer 'concern' questions about privacy means the market is the most efficient mechanism to allow these consumers to find their privacy preferences.		Empirical work on privacy needs for regulations and public policy should be measured within the specific context and based on the vulnerability of the users.

In fact, further testing around Westin's privacy concern measurements also illustrates this ambiguity in the evaluative term *concern*. One study found even respondents labeled "unconcerned" rated the vignettes about the use of their data online as not meeting privacy expectations.[16] The same study found that Westin's categorizations may actually capture respondents trust in business—those who are labeled unconcerned have strong privacy expectations but trust businesses to

[16] the westin categorization explained only 15% of the variance in privacy expectations as compared to the factors in the vignette. Martin and nissenbaum, "measuring privacy: an empirical test using context to expose confounding variables" 211; *see also* Martin and Nisenbaum, Martin and Nisenbaum, "measuring privacy: an empirical test using context to expose confounding variables," , 177 ("Westin's privacy categories proved relatively unimportant in relation to contextual elements in privacy judgments. Even privacy 'unconcerned' respondents rated the vignettes as not meeting privacy expectations on average, and respondents across categories had a common vision of what constitutes a privacy violation.").

protect their privacy in general.[17] This connection is actually well-understood: greater institutional trust is found to reduce general concerns about privacy (Rohm and Milne 2004; Xu, Wang, and Teo 2005). So respondents rating a low concern about privacy is partially explained by how much they trust business to not violate their privacy: respondents may care a great deal about privacy violations but do not think firms will or violate their privacy.

The point for Schaeffer and Presser – the scholars who study survey design -- is that this type of ambiguity drives variance in answers and that the goal should be "to identify wording for both [objective and evaluative components] that will be easy to understand *and that will be understood similarly by all respondents"* [emphasis added].

Ambiguity does not mean the survey instruments are wrong or should not be used – although some could be improved. However, the ambiguity and level of analysis ('concern for privacy') is why questions about dispositions do not directly translate into privacy judgments about specific data flows. The fact that respondents vary in how they answer general questions about privacy or questions about privacy concerns is expected and says little about specific privacy preferences or needs within a specific context. Surveys designed to take general 'temperature' questions – such as whether we trust congress or whether we trust business – are not designed to translate into specific judgments about market actions. As summarized by Acquisti et al "inconsistencies between broad attitudes and specific behaviors are well-recognized in the literature predating privacy decision making" (Acquisti, Brandimarte, and Loewenstein 2020, 749). Which brings us to the last myth, the privacy paradox.

2.3 Myth #3: People behave according to the privacy paradox.

The privacy paradox is the claim that consumers' stated privacy preferences, needs, and expectations in surveys (paradoxically) diverge from their actual behavior in the market. Privacy paradox "reflects the observed phenomenon that often while consumers express a desire for privacy when asked about it, it appears they are willing to share their data very readily in a way which seems to contradict this."[18] The claim helps to explain why people state clear privacy judgments in surveys (to not have location stored, to not have their information sold to data brokers, to not

[17] ("Westin's categorization may be more a factor of institutional trust . . . with privacy unconcerned having a positive trust in websites generally … whereas privacy fundamentalists have a distrust in websites generally . . ."(Martin and Nissenbaum 2015).
[18] https://www.nber.org/system/files/chapters/c14781/revisions/c14781.rev1.pdf tucker.

have their data later used for targeted advertising, etc), yet consumers still go online where firms are violating their privacy.

As summarized by Alashoor et al, evidence of the privacy paradox "abounds" in that clear, observed evidence is readily available (Alashoor et al. 2023). For example,

> **"**Do people really care about their privacy? Surveys show that privacy is a primary concern for citizens in the digital age. On the other hand, individuals reveal personal information for relatively small rewards…This inconsistency of privacy attitudes and privacy behaviour is often referred to as the "privacy paradox" (Kokolakis 2017, 122).

When a survey instrument does not perfectly predict 'privacy behavior,' advocates of the privacy paradox frame the individual as at fault inconsistent and argue that people's behavior in the market – continuing to go online, to use a phone – is a better indicator of their privacy needs, preferences, and expectations.[19]

The privacy paradox is useful for industry in order to explain academic research and national surveys showing people have specific privacy expectations, needs, and preferences about how their data is collected, shared, used within a specific context. These privacy judgments in surveys can run counter to current business models. And, importantly, this disconnect between consumer privacy needs and industry practices may suggest regulation or public policy action is needed to protect consumers. Industry needs 'privacy paradox' framing so as to not be asked to explain why firms continually violate privacy.[20] The answer, according to those espousing the privacy paradox, is that consumers act willingly and paradoxically against their stated interests.

As to public policy, privacy paradox scholars and experts in congressional testimony, shift the focus from empirical work measuring specific privacy judgments in favor of consumers' decision to continue to go online. Solove refers to this as the "behavior valuation argument" from industry – that people's behavior is what we should focus on and, therefore, since people still go online, less regulation is needed (Solove 2021). For example, congressional testimony by Adam Thierer makes such a claim:

[19] Interestingly, faith in general 'privacy concern' survey instruments that are used to show variance in how individuals answer general questions about privacy turns to dismissal of more specific measurements of privacy needs, preferences, and expectations – where the findings undermine current business models.
[20] For example, using historical data for behaviorally targeted ads is consistently found to be a privacy violation (Martin 2015). However, firms continue to rely on the personalized ads as a more profitable product line (compared to other types of ads) and the privacy paradox argument allows firms to plausibly ignore such survey findings.

> What consumers claim to care about and what they actually do in the real-world are often two very different things. In the real-world, people balance privacy and security alongside many other values, including choice, convenience, cost, and more. This leads to the so-called ``privacy paradox, or the problem of many people saying one thing and doing quite another when it comes to privacy matters.[21]

As noted by Kokolakis, continued proof of the privacy paradox in research encourages firms to increase the collection and use of personal information (2017). Consumer-facing firms, marketers, and advertising advocacy groups use the privacy paradox to justify their current data practices, while also reporting data that shows that consumers overwhelmingly find such practices problematic and creepy (Martin 2020).

2.3.1 Critiques.

Research on the privacy paradox splits into two camps. First, research seeks to demonstrate the privacy paradox by showing how respondents answer survey questions and then posit these answers as counter to actual behavior (e.g., Strahilevitz and Kugler 2016 Norberg, Horne, and Horne 2007).

Other researchers take the privacy paradox as a given and seek to explain why consumers behave in a way seen as counter to their survey answers. These researchers focus on psychological and economic factors (Acquisti 2020) or mood (Alashoor et al. 2023) that interfere with the individual making choices that match their general privacy concern measurement. For example, people may discount potential future harms when sharing information (Acquisti & Grossklags, 2003) or just be too tired (Alashoor et al. 2023). In general, this line of research takes the paradox or gap between general privacy dispositions and specific privacy judgments and seeks to identify "limitations in consumers' cognitive ability, or their susceptibility to behavioral heuristics and decision biases" (Adjerid, Peer, and Acquisti 2018) which impact consumer decisions (Brandimarte et al., 2013).

Privacy paradox scholarship regularly centers the consumer as responsible for why general survey questions about privacy dispositions or concerns do not predict specific privacy decisions (usually a decision to disclose information to a firm or to a researcher). Here I wish to take a different approach and point out *how odd it would be if general privacy concerns or attitudes predicted specific behavior.* Where many scholars seek to place the consumer at fault for when "association

[21] https://www.congress.gov/event/114th-congress/senate-event/lc37723/text?q=%7b%22search%22%3a%22%5c%22privacy+paradox%5c%22%22%7d&s=1&r=2

between stated privacy concerns and disclosure behaviors is significantly weakened" (Alashoor et al. 2023), here we can see how it was a myth to believe these general dispositions would ever predict privacy actions.

2.3.2 Measuring Privacy in Surveys

Privacy paradox research measures respondents stated privacy judgments in surveys in comparison to people's privacy actions in the market.[22] In this way, two measurements of privacy are important. The researcher (1) must measure specific stated privacy judgments (privacy preferences, needs, and expectations) and (2) identify if or how those stated judgments match actual choices in the market. And most privacy paradox scholarship, I argue below, misses on both fronts.

What does it mean to make a meaningful privacy judgment? What factors do you need clarity on before judging a data flow is appropriate, meets expectations, is a preference, or is not ok? To capture responses that speak to consumers' expectations, approval, and preference requires information about the context of data collection, actors involved (who sends, collects, accesses the data), the conditions under which data is transmitted, and the goals and purposes of the data use. One way to measure privacy judgments too generally is to focus only a limited number of parameters – e.g., the type of information (e.g., ratings of 'sensitive' information, etc) or the actor collecting the data (Nissenbaum 2010). So, asking only about location data without explaining the context in which it is shared, who receives the data, what inferences can be created, and how the data will be used will be of limited utility. Similarly asking about a specific actor – the government or a gaming app – would also not provide enough information to capture a person's specific privacy need in a particular context.

Solove refers to the comparison of general privacy concerns to specific privacy behavior as a logical fallacy (Solove 2021), however social scientists do measure general attitudes and dispositions compared to, more specific, yet related behaviors. For example, we regularly measure general trust and even institutional trust: trust in U.S. banking (Fungáčová, Hasan, and Weill 2019), trust in government (Chanley, Rudolph, and Rahn 2000), or trust in the supreme court (Gibson, Caldeira, and Spence 2003). These general institutional trust measurements can be connected to more specific trust judgments, e.g., trust in a congress person, or a specific trust action, e.g., voting for that congress person.

[22] For example "This dichotomy between people's self-reported mental states (attitudes, concerns, desires, etc.) regarding privacy and their actual behaviors. This dichotomy is known as the privacy paradox,…" (Acquisti et al. 2020, p. 749).

But general institutional trust does not predict someone's actions *and it is not designed to be such a measurement.* Research on trust, for example, measures institutional trust in business as well as trust in a specific firm for a particular purpose (Pirson, Martin, and Parmar 2014). Institutional trust is then a control variable for most analysis i that someone's institutional trust in business may explain a small portion of their specific trust in a firm, but the main drivers of trust in a specific organization is the ability and integrity behavior of that organization. Pavlou and Gefen (2004), for example, found that 'trust in the community of sellers" impacts intention to transact but does not fully explain trust in a particular firm. And Bhattacherjee (2002) validated a measurement of institutional trust and measured it had a statistically significant impact on willingness to transact – but again only had moderate explanatory power. These were not surprising findings – institutional trust is not expected to predict a specific trust judgment in a firm. Firm actions (and the perception of those action) drive specific trust judgments and consumer trust actions.

Yet, privacy paradox scholarship continues to return to general privacy concern measurements as if these should predict behavior. For example, an article by Speikermann et al cited by many (e.g., Norberg, Horne, and Horne 2007; Adjerid, Peer, and Acquisti 2018; Hargittai and Marwick 2016) as evidence of the privacy paradox shows how a general privacy concern survey does not perfectly predict whether respondents disclosed certain information to a chat bot (Spiekermann, Grossklags, and Berendt 2001). Kokolakis rightly highlights an article usually cited as examining the privacy paradox but where the author (Hughes-Roberts 2013) concluded "that a general statement of user concern is not a valid indicator of privacy behaviour within the [social] network" and questioned the utility of of using surveys to establish a privacy paradox (Kokolakis 2017).

General measurements are not *useless*, but do have a particular purpose within social science research. In fact, more work should be done similar to other disciplines to understand not only how general privacy attitudes or concerns impact privacy actions but also how specific actions of firms and industry and possibly regulations drive privacy behavior.

2.3.3 *Measuring Privacy in Market*

Which brings us to the second phenomenon to be measured: privacy actions in the market. To capture consumers' operationalizing their privacy judgment within a market action or an experiment – where economic preference is meaningfully reflected in an individual's choice -- the individual must not only understand the

important parameters of the privacy decision at issue (as noted above – context, actors, transmission principle, purpose or use, etc), but also have the opportunity to make a meaningful choice that is a reflection of their privacy judgment. To have an opportunity, consumers would need an option that matches specific privacy needs and the ability to easily choose that preferred option.

However, privacy paradox scholarship and testimony continues to return to mere disclosure decisions as an action that gives up privacy. So, we have statements such as:

> On the one hand, users express concerns about the handling of their personal data and report a desire to protect their data, whereas at the same time, they not only voluntarily give away these personal data by posting details of their private life in social networks or using fitness trackers and online shopping websites which include profiling functions, but also rarely make an effort to protect their data actively, for example through the deletion of cookies on a regular basis or the encryption of their e-mail communication. ….(Gerber, Gerber, and Volkamer 2018, emphasis added).

Note that evidence of disregarding privacy or giving away privacy is using a social network, fitness tracker, or just online shopping. Importantly, mere disclosure of information is not enough to indicate that someone is 'giving up' or does not prioritize privacy since people disclose information all the time while expecting privacy norms will be respected. The consumer behavior being measured in the market is mistakenly being framed as relinquishing privacy when the individual is merely sharing information with a company to be used to receive products and services.

Such a strong version of the privacy paradox can be seen in statements such as "privacy paradox, in which users voluntarily renounce their data in exchange for services, products, and benefits."(Luz Da Rocha and Chimenti 2022) or in a well-cited summary of the privacy paradox where Barth et al (2017) define privacy behavior as 'actual information disclosure.'

Market actions reveal consumer preferences about quality and price under particular circumstances. The actors must be able to find each other, know that they are negotiating and over what, have similar amounts of information about the data practices, have options that closely match their preferences with minimal transaction costs, etc.

The focus on consumers as acting paradoxically – as having a stated preferences but not choosing that same preference in practice – is predicated on an assumption that those options easily exist either across firms or within a particular firm.

2.3.4 Blame consumer

The final oddity in privacy paradox studies is placing the onus of responsibility on consumers as privacy arbiters in the face of an obscure and hostile market. Normally, researchers who hypothesize that a survey or experiment will predict a particular outcome *do not blame the respondents* when their hypothesis is not supported by data. So, researchers may hypothesize that how people answer Westin's 'privacy concern' questions will predict whether respondents share location data with a mapping app – but it could also be that (a) the survey question does not capture specific privacy preference, needs, and expectations around that particular context and (b) disclosing location data to a mapping app was done without the requisite knowledge (and therefore not a meaningful 'choice'). Normally, researchers regroup and attempt to understand why that particular survey question was not significant or important in explaining market behavior (if it was). Did they measure the same phenomenon? Was the question ambiguous? Were the consumers able to make a choice that matches their preferences, needs, or expectations? Privacy paradox scholarship is unique in blaming the respondent when a general disposition measurement does not predict specific behavior.[23]

3. IMPLICATIONS AND CONCLUSION

Thus far I have identified two mistake assumptions in privacy research: defining privacy as concealment and focusing on the consumer as the privacy negotiator in the market. I illustrated how current mythes about privacy in the market make some combination of these mistakes. The tradeoff myth relies on privacy as concealment whereas the unconcerned consumer myth blames the consumer for a poorly designed survey. The privacy paradox myth combines both in blaming the consumer for continuing to go online considering their stated privacy needs and using mere engagement as evidence that those consumers 'gave up' privacy.

Two streams of research are promising in this area to better understand why market action is not indicative of consumer privacy needs, preferences, and

[23] Or even when a survey is more specific but about a different phenomenon. An example would be asking students about their preferences around crypto-wallets in a survey and comparing their answer to whether the student provided an email to researchers for free pizza (Athey, Catalini, and Tucker, n.d.).

expectations. First, is in better understanding the privacy needs, preferences, and expectations of individual within specific contexts. For example, studying the creation of inferences and targeted advertising (Schoenebeck et al. 2024; Martin, Nissenbaum, and Shmatikov 2024) or specifically the creation and use of emotion inferences at work (Roemmich, Schaub, and Andalibi 2023). These studies focus on specific social domains and provide important parameters for respondents to make meaningful privacy judgments.

Similarly, Colnago, Cranor, and Acquisti (2023) provide an excellent example of designing more nuanced, specific survey questions to better capture consumer privacy needs, preferences that map onto consumer behavior. After eliciting actual consumer behavior, the authors asked general privacy attitude and concern questions, which did not map nicely onto behaviors, and then more specific preferences, which did map onto behaviors.[24] The authors were able to avoid consumers appears 'inconsistent' by not only removing the ambiguity in the survey prompts but also by better matching the specificity of the questions to the specificity of the action.

Third, operationalizing privacy decision in the market need not fixate on disclosure decisions. For example, research attempting to better understand market action includes work on younger people who use different ways of protecting information "such as using pseudonyms and giving false information (Miltgen & Peyrat-Guillard, 2014), restricting access to their profiles and adjusting their privacy settings (boyd & Hargittai, 2010), limiting friendship requests, and deleting tags and photos (Young & Quan-Haase, 2013)" as noted by Kokolakis.[25]

Finally, research can relax the degree to which the consumer is (incorrectly) centered as the great privacy arbiter in the market. A concerning trend is to

[24] An example of the more specific prompt and behavior would be "I want to only have financial information with companies I trust" (preference) and "Only disclosed financial information with companies that are well established and reputable" (action). An example of the more general survey questions used that did not map onto behavior include "I think privacy is important for society" (Colnago, Cranor, and Acquisti 2023)

[25] For example, "Tufekci (2008) reports the results of a questionnaire survey aiming to study students' self-disclosure behaviour in SNSs. The study found little to no relationship between online privacy concerns and information disclosure. Another interesting result is that students manage their concerns about unwanted audience by adjusting the visibility of information, but not by regulating the levels of disclosure." From Kokolakis:

measure the degree to which consumers take protective action to combat the persistent attempt to collect, use, and share their data by tech companies. For example, privacy paradox scholarship may measure if consumers take sufficient counter-measures to combat the increasingly intrusive collection, sharing and use of their data. For example, "In other words, although people say they reject OBA, they take few measures to protect their data from it." (Boerman, Kruikemeier, and Zuiderveen Borgesius 2017). A noted departure of this focus on what the individual is doing incorrectly is by Ari Waldman who focuses on the design of dark patterns that may get in the way of making decisions in our best interest (Waldman 2020). Similarly, Kokolakis posits designed frictions that could be in the way of consumers making decisions that match their privacy preference, expectations, and needs. Alternatively, researchers could study why firms in an antagonistic relationship with users? Why is it so difficult for users to enact their privacy preferences, needs, and expectations?

References

Acquisti, Alessandro. 2023. "The Economics of Privacy at a Crossroads." *Economics of Privacy. University of Chicago Press*.

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. 2020. "Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age." *Journal of Consumer Psychology* 30 (4): 736–58.

Acquisti, Alessandro, and Ralph Gross. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." In , 36–58. Springer.

Acquisti, Alessandro, Leslie K John, and George Loewenstein. 2013. "What Is Privacy Worth?" *The Journal of Legal Studies* 42 (2): 249–74.

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. 2016. "The Economics of Privacy." *Journal of Economic Literature* 54 (2): 442–92.

Adjerid, Idris, Eyal Peer, and Alessandro Acquisti. 2018. "Beyond the Privacy Paradox: Objective versus Relative Risk in Privacy Decision Making." *MIS Quarterly* 42 (2): 465–88.

Alashoor, Tawfiq, Mark Keil, H Jeff Smith, and Allen R McConnell. 2023. "Too Tired and in Too Good of a Mood to Worry about Privacy: Explaining the Privacy Paradox through the Lens of Effort Level in Information Processing." *Information Systems Research* 34 (4): 1415–36.

Al-Jabri, Ibrahim M, Mustafa I Eid, and Amer Abed. 2019. "The Willingness to Disclose Personal Information: Trade-off between Privacy Concerns and Benefits." *Information & Computer Security* 28 (2): 161–81.

Athey, Susan, Christian Catalini, and Catherine Tucker. n.d. "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk." *MIT Sloan Research Paper* 5196.

Beresford, Alastair R, Dorothea Kübler, and Sören Preibusch. 2012. "Unwillingness to Pay for Privacy: A Field Experiment." *Economics Letters* 117 (1): 25–27.

Bhargava, Vikram R, and Manuel Velasquez. 2021. "Ethics of the Attention Economy: The Problem of Social Media Addiction." *Business Ethics Quarterly* 31 (3): 321–59.

Bloustein, Edward J. 1964. "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser." *NYUL Rev.* 39:962.

Boerman, Sophie C, Sanne Kruikemeier, and Frederik J Zuiderveen Borgesius. 2017. "Online Behavioral Advertising: A Literature Review and Research Agenda." *Journal of Advertising* 46 (3): 363–76.

Boerman, Sophie C, and Edith G Smit. 2023. "Advertising and Privacy: An Overview of Past Research and a Research Agenda." *International Journal of Advertising* 42 (1): 60–68.

Brunton, Finn, and Helen Nissenbaum. 2011. "Vernacular Resistance to Data Collection and Analysis: A Political Theory of Obfuscation." *First Monday* 16 (5).

Calo, M Ryan. 2011. "Boundaries of Privacy Harm, The." *Ind. LJ* 86:1131.

Calo, Ryan. 2015. "Privacy and Markets: A Love Story." *Notre Dame L. Rev.* 91:649.

Chander, Anupam, Margot E Kaminski, and William McGeveran. 2020. "Catalyzing Privacy Law." *Minn. L. Rev.* 105:1733.

Chanley, Virginia A, Thomas J Rudolph, and Wendy M Rahn. 2000. "The Origins and Consequences of Public Trust in Government: A Time Series Analysis." *Public Opinion Quarterly* 64 (3): 239–56.

Chen, Chaoran, Weijun Li, Wenxin Song, Yanfang Ye, Yaxing Yao, and Toby Jia-Jun Li. 2024. "An Empathy-Based Sandbox Approach to Bridge the Privacy Gap among Attitudes, Goals, Knowledge, and Behaviors." In , 1–28.

Citron, Danielle Keats. 2018. "Sexual Privacy." *Yale Law Journal* 128:1870–1960.

———. 2022. "Intimate Privacy's Protection Enables Free Speech." *J. Free Speech L.* 2:3.

Citron, Danielle Keats, and Daniel J Solove. 2022. "Privacy Harms." *BUL Rev.* 102:793.

Cofone, Ignacio N, and Adriana Z Robertson. 2017. "Privacy Harms." *Hastings LJ* 69:1039.

Cohen, Julie E. 2012. "What Privacy Is For." *Harvard Law Review* 126:1904–33.

Colnago, Jessica, Lorrie Faith Cranor, and Alessandro Acquisti. 2023. "Is There a Reverse Privacy Paradox? An Exploratory Analysis of Gaps Between Privacy Perspectives and Privacy-Seeking Behaviors." *Proceedings on Privacy Enhancing Technologies* 1:455–76.

Colnago, Jessica, Lorrie Faith Cranor, Alessandro Acquisti, and Kate Hazel Stanton. 2022. "Is It a Concern or a Preference? An Investigation into the Ability of Privacy Scales to Capture and Distinguish Granular Privacy Constructs." In , 331–46.

DeCew, Judith Wagner. 1986. "The Scope of Privacy in Law and Ethics." *Law and Philosophy*, 145–73.

Dinev, Tamara, and Paul Hart. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions." *Information Systems Research* 17 (1): 61–80.

Ellis Davidson, Hilda Roderick. 1969. "The Legend of Lady Godiva." *Folklore* 80 (2): 107–21.

Fungáčová, Zuzana, Iftekhar Hasan, and Laurent Weill. 2019. "Trust in Banks." *Journal of Economic Behavior & Organization* 157:452–76.

Gavison, Ruth. 1980. "Privacy and the Limits of Law." *The Yale Law Journal* 89 (3): 421–71.

Gerber, Nina, Paul Gerber, and Melanie Volkamer. 2018. "Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior." *Computers & Security* 77:226–61.

Gibson, James L, Gregory A Caldeira, and Lester Kenyatta Spence. 2003. "Measuring Attitudes toward the United States Supreme Court." *American Journal of Political Science* 47 (2): 354–67.

Gunawan, Johanna, David Choffnes, Woodrow Hartzog, and Christo Wilson. 2024. "Design Loyalty Approaches for Dark Patterns." https://www.conpro24.ieee-security.org/papers/gunawan-conpro24.pdf.

Hallam, Cory, and Gianluca Zanella. 2017. "Online Self-Disclosure: The Privacy Paradox Explained as a Temporally Discounted Balance between Concerns and Rewards." *Computers in Human Behavior* 68:217–27.

Hargittai, Eszter, and Alice Marwick. 2016. "'What Can I Really Do?' Explaining the Privacy Paradox with Online Apathy." *International Journal of Communication* 10:21.

Hartzog, Woodrow. 2011. "Chain-Link Confidentiality." *Ga. L. Rev.* 46:657.
Hayek, Friedrich August. 1945. "The Use of Knowledge in Society." *The American Economic Review* 35 (4): 519–30.
Hermalin, Benjamin E, and Michael L Katz. 2006. "Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy." *Quantitative Marketing and Economics* 4 (3): 209–39.
Hildebrandt, Mireille. 2019. "Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning." *Theoretical Inquiries in Law* 20 (1): 83–121.
Hoofnagle, Chris Jay, and Jennifer M Urban. 2014. "Alan Westin's Privacy Homo Economicus." *Wake Forest Law Review* 49:261.
Hughes-Roberts, Thomas. 2013. "Privacy and Social Networks: Is Concern a Valid Indicator of Intention and Behaviour?" In , 909–12. IEEE.
Kim, Dongyeon, Kyuhong Park, Yongjin Park, and Jae-Hyeon Ahn. 2019. "Willingness to Provide Personal Information: Perspective of Privacy Calculus in IoT Services." *Computers in Human Behavior* 92:273–81.
Kokolakis, Spyros. 2017. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon." *Computers & Security* 64:122–34.
Lobschat, Lara, Benjamin Mueller, Felix Eggers, Laura Brandimarte, Sarah Diefenbach, Mirja Kroschke, and Jochen Wirtz. 2021. "Corporate Digital Responsibility." *Journal of Business Research* 122:875–88.
Luz Da Rocha, Roger, and Paula Chimenti. 2022. "Consumer Concerns of Personal Data and Privacy: A Systematic Review." In , 2022:18207. Academy of Management Briarcliff Manor, NY 10510.
Malhotra, Naresh K, Sung S Kim, and James Agarwal. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model." *Information Systems Research* 15 (4): 336–55.
Martin, Kirsten. 2013. "Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online." *First Monday* 18 (12).
———. 2015. "Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online." *Journal of Public Policy & Marketing* 34 (2): 210–27. http://dx.doi.org/10.1509/jppm.14.139.
———. 2016a. "Data Aggregators, Consumer Data, and Responsibility Online: Who Is Tracking Consumers Online and Should They Stop?" *The Information Society* 32 (1): 51–63.
———. 2016b. "Understanding Privacy Online: Development of a Social Contract Approach to Privacy." *Journal of Business Ethics* 137 (3): 551–69. https://doi.org/10.1007/s10551-015-2565-9.
———. 2020. "Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms." *Business Ethics Quarterly* 30 (1): 65–96.
———. 2022. "Manipulation, Choice, and Privacy." *North Carolina Journal of Law & Technology* 23 (3): 452–524. https://scholarship.law.unc.edu/ncjolt/vol23/iss3/2/.

Martin, Kirsten, and Helen Nissenbaum. 2015. "Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables." *Columbia Science and Technology Law Review* 18:176.

———. 2020. "What Is It About Location?" *Berkeley Technology Law Journal* 35 (1): 252–323.

Martin, Kirsten, Helen Nissenbaum, and Vitaly Shmatikov. 2024. "No Cookies For You!: Evaluating The Promises Of Big Tech's 'Privacy-Enhancing'Techniques." *Georgetown Law Technology Review (Forthcoming)*.

McDonald, Nora, and Andrea Forte. 2020. "The Politics of Privacy Theories: Moving from Norms to Vulnerabilities." In , 1–14.

Murphy, Richard S. 2017. "Property Rights in Personal Information: An Economic Defense of Privacy." In *Privacy*, 43–79. Routledge.

Nagel, Thomas. 1998. "Concealment and Exposure." *Philosophy & Public Affairs* 27 (1): 3–30.

Nissenbaum, Helen. 1997. "Toward an Approach to Privacy in Public: Challenges of Information Technology." *Ethics & Behavior* 7 (3): 207–19.

———. 1998. "Protecting Privacy in an Information Age: The Problem of Privacy in Public." *Law and Philosophy* 17 (5): 559–96.

———. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Norberg, Patricia A, Daniel R Horne, and David A Horne. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors." *Journal of Consumer Affairs* 41 (1): 100–126.

Obar, Jonathan A, and Anne Oeldorf-Hirsch. 2020. "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services." *Information, Communication & Society* 23 (1): 128–47.

Pirson, Michael, Kirsten Martin, and Bidhan Parmar. 2014. "Public Trust in Business and Its Determinants." In *Public Trust in Business*, edited by Jared D Harris, Brian Moriarty, and Andrew C Wicks, 116–52. Cambridge University Press.

Posner, Richard A. 1981. "The Economics of Privacy." *The American Economic Review* 71 (2): 405–9.

———. n.d. "The Right of Privacy'(1978)." *Georgia Law Review* 12:393.

Regan, Priscilla M. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy*. Univ of North Carolina Press.

———. 2011. "Response to Bennett: Also in Defense of Privacy." *Surveillance & Society* 8 (4): 497–99.

Reidenberg, Joel R. 2014. "Privacy in Public." *University of Miami Law Review* 69:141.

Richards, Neil. 2015. *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. Oxford University Press, USA.

Richards, Neil, and Woodrow Hartzog. 2018. "The Pathologies of Digital Consent." *Wash. UL Rev.* 96:1461.

———. 2021. "A Duty of Loyalty for Privacy Law." *Wash. UL Rev.* 99:961.

Richards, Neil M, and Woodrow Hartzog. 2020. "A Duty of Loyalty for Privacy Law." *Available at SSRN*.

Roemmich, Kat, and Nazanin Andalibi. 2021. "Data Subjects' Conceptualizations of and Attitudes toward Automatic Emotion Recognition-Enabled Wellbeing

Interventions on Social Media." *Proceedings of the ACM on Human-Computer Interaction* 5 (CSCW2): 1–34.

Roemmich, Kat, Florian Schaub, and Nazanin Andalibi. 2023. "Emotion AI at Work: Implications for Workplace Surveillance, Emotional Labor, and Emotional Privacy." In , 1–20.

Rohm, Andrew J, and George R Milne. 2004. "Just What the Doctor Ordered: The Role of Information Sensitivity and Trust in Reducing Medical Information Privacy Concern." *Journal of Business Research* 57 (9): 1000–1011.

Schaeffer, Nora Cate, and Stanley Presser. 2003. "The Science of Asking Questions." *Annual Review of Sociology* 29 (1): 65–88.

Schnadower Mustri, Eduardo, Idris Adjerid, and Alessandro Acquisti. 2023. "Behavioral Advertising and Consumer Welfare: An Empirical Investigation." *Available at SSRN 4398428*.

Schoenebeck, Sarita, Cami Goray, Amulya Vadapalli, and Nazanin Andalibi. 2024. "Sensitive Inferences in Targeted Advertising." *Northwestern Journal of Technology and Intellectual Property* 21 (2): 1.

Scholz, Lauren Henry. 2019. "Privacy Remedies." *Ind. LJ* 94:653.

Shilton, Katie, Emanuel Moss, Sarah A Gilbert, Matthew J Bietz, Casey Fiesler, Jacob Metcalf, Jessica Vitak, and Michael Zimmer. 2021. "Excavating Awareness and Power in Data Science: A Manifesto for Trustworthy Pervasive Data Research." *Big Data & Society* 8 (2): 20539517211040759.

Sivan-Sevilla, Ido, Helen Nissenbaum, and Patrick T. Parham. 2022. "Public Comment for FTC's Commercial Surveillance ANPR." Preprint. Open Science Framework. https://doi.org/10.31219/osf.io/wjr5z.

Smith, H Jeff, Sandra J Milberg, and Sandra J Burke. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices." *MIS Quarterly*, 167–96.

Solove, Daniel J. 2021. "The Myth of the Privacy Paradox." *Geo. Wash. L. Rev.* 89:1.

Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. 2001. "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior." In , 38–47. ACM.

Stigler, George J. 1961. "The Economics of Information." *Journal of Political Economy* 69 (3): 213–25.

———. 1980. "An Introduction to Privacy in Economics and Politics." *The Journal of Legal Studies* 9 (4): 623–44.

Strandburg, Katherine J. 2010. "Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change." *Md. L. Rev.* 70:614.

Susser, Daniel. 2016. "Information Privacy and Social Self-Authorship." *Techne: Research in Philosophy & Technology* 20 (3).

Susser, Daniel, Beate Roessler, and Helen Nissenbaum. 2019. "Technology, Autonomy, and Manipulation." *Internet Policy Review* 8 (2).

Take, Kejsi, Kevin Gallagher, Andrea Forte, Damon McCoy, and Rachel Greenstadt. 2022. "'It Feels like Whack-a-Mole': User Experiences of Data Removal from People Search Websites." *Proceedings on Privacy Enhancing Technologies* 2022 (3).

Tsai, Janice Y, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study." *Information Systems Research* 22 (2): 254–68.

Tufekci, Zeynep. 2008. "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites." *Bulletin of Science, Technology & Society* 28 (1): 20–36.

Urban, Jennifer M, and Chris Jay Hoofnagle. 2014. "The Privacy Pragmatic as Privacy Vulnerable." In .

Waldman, Ari Ezra. 2018. *Privacy as Trust: Information Privacy for an Information Age*. Cambridge University Press.

———. 2020. "Cognitive Biases, Dark Patterns, and the 'Privacy Paradox.'" *Current Opinion in Psychology* 31:105–9.

Warren, Samuel D, and Louis D Brandeis. 1890. "The Right to Privacy." *Harvard Law Review*, 193–220.

Westin, Alan. 1991. "Harris Louis & Associates. Harris-Equifax Consumer Privacy Survey." Tech. rep, Conducted for Equifax Inc. 1,255 adults of the US public.

Xu, Heng, Tamara Dinev, Jeff Smith, and Paul Hart. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances." *Journal of the Association for Information Systems* 12 (12): 1.

Xu, Heng, Xin Robert Luo, John M Carroll, and Mary Beth Rossen. 2011. "The Personalization Privacy Paradox: An Exploratory Study of Decision Making Process for Location-Aware Marketing." *Decision Support Systems* 51 (1): 42–52.

Xu, Heng, Hock-Hai Teo, Bernard CY Tan, and Ritu Agarwal. 2009. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services." *Journal of Management Information Systems* 26 (3): 135–74.

Xu, Heng, Hao Wang, and Hock-Hai Teo. 2005. "Predicting the Usage of P2P Sharing Software: The Role of Trust and Perceived Risk." In *System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference On*, 201a–201a. IEEE.

Zhang, Shikun, Yuanyuan Feng, Lujo Bauer, Lorrie Faith Cranor, Anupam Das, and Norman Sadeh. 2021. "'Did You Know This Camera Tracks Your Mood?': Understanding Privacy Expectations and Preferences in the Age of Video Analytics." *Proceedings on Privacy Enhancing Technologies*.