

Marketing managers should expect less access to data and therefore invest in trustful relationships where customers voluntarily opt for less privacy.



# Ghosts in the Dark: How to Prepare for Times of Hyper-Privacy

Felipe Thomaz

## KEYWORDS

**Dark Web, Privacy, Privacy Calculus, Privacy Paradox, Personalization**

## THE AUTHOR

### **Felipe Thomaz**

Associate Professor of Marketing, Saïd Business School, University of Oxford, England  
[Felipe.Thomaz@sbs.ox.ac.uk](mailto:Felipe.Thomaz@sbs.ox.ac.uk)

## **A hidden digital romping ground is thriving in the dark**

✗ The web is a dynamic, complex, and rapidly evolving environment, with literal fortunes made and lost as the waves of change give rise to different business models. However, this complexity is deeper than immediately obvious. Apart from the surface web that most of us experience every day, there is a separate, hidden layer called the dark web. Here the websites are unindexed, access is only possible via Tor, a specialized browser, and communications are usually encrypted. Every aspect of the dark web is designed to provide privacy to its users. If you've heard of the dark web before, then it might have been in discussions related to the number of illicit businesses operating there. It is the home of hackers, drug markets, data brokers, and human traffickers. However, it also serves as a safe haven for whistleblowers, activists, and journalists, as well as citizens from countries where communication is either restricted or monitored. Altogether, it is a place built for individuals who are exceptionally incentivized to be digitally invisible.

## **The dark web – a dorado for privacy**

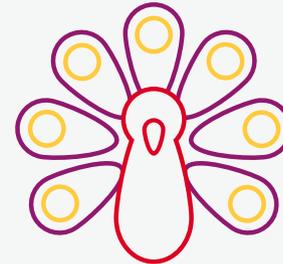
✗ However, the dark web has its bright sides because it also exists as an unregulated testbed for technologies that we will eventually experience on the surface: WhatsApp, as an example, provides similar end-to-end encrypted communication, and surface-web consumers start gaining experience with bitcoin, whereas, in the dark web, they use it for a shadow economy with a GDP larger than Peru's, along with several other cryptocurrencies. That provides us with a useful place to study consumer privacy and have a view of what the surface world might look like under an extreme level of consumer data protection. And the extent of that protection is astonishing. When I investigated my own digital footprint

FIGURE 1 > Marketing to Ghosts and Buffs

### Ghosts

Consumers who generally deny access to their personal digital information.

- > Explicit data collection on permission
- > Transparency
- > Anonymized aggregate profiles
- > Mass-personalization



### Buffs

Consumers rendering their digital essence “naked” by willing to give permission to track, record, use, and share information like purchase and site visit histories.

- > Similar to today’s digital consumers
- > Implicit data collection like tracking
- > Hyper-individualized profile
- > Hyper-personalization

on the surface web, I found close to 5000 tracked variables across data aggregators, ranging from absurd guesses to oddly specific details that have been accumulated over the past decade. Conversely, the average “persistent” dark web user – one that decides to keep the same persona for more than a single burst of use – had eight data points. Yet, most smart dark web users who forego this persistent personal branding could choose to leave essentially zero trace of their existence. And with that, they become invisible. Ghosts.

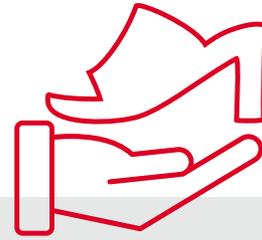
#### The dark web’s privacy – a nightmare for marketers

✗ This reality should be terrifying to anyone relying on the modern marketing machinery that fuels much of today’s business growth and competitive edge, as all of it relies on abundant information. Lookalike matching, collaborative filtering, precision targeting, audience controls: all of it disappears if everyone is a ghost. Even our best customers will look like never-before-seen individuals until they decide to reveal themselves, by logging in or entering ID information, for instance. And as a result, marketers would be reduced to pre-information-age tactics, reliant on population averages, and at best, using unsupervised machine learning techniques, like clustering.

**The privacy calculus: Ghosts or Buffs?** ✗ But not everything is ghosts, doom and gloom. Ghosting is a consumer choice. This choice between privacy and disclosure is called the privacy calculus. If there is trust and a worthwhile value exchange, consumers might be willing to share their data and not enact all of the hyper-privacy available to them, continuing to give marketers a full view of their behaviors and preferences. We call these customers “Buffs” (see Figure 1). For Buffs, marketers will have the full modern array of marketing and predictive analytics available, and, provided they are doing their jobs well, one can imagine that this can only lead to higher profitability and retention rates.

#### Nudging consumers against the ghosting option to share behavioral information and preferences

✗ To explain how consumers can be convinced to be less secretive, I like to use an analogy. The exercise is simple: First, imagine your ideal lover/partner. This person knows you inside and out. Somehow, they always say the right thing and intuit exactly what you need, when you need it. That is one set of behaviors and one type of relationship. Now consider an alternative: This person has gone through your rubbish bin to try to figure out what you’ve been up to. They opened



## BOX 1

## Soft hyper-personalization: Act like a caring partner, not a stalker

If you run a shoe retailer, you are well within your right and within the expectation of remembering your customer's shoe size, as well as their color/brand/designer preferences. You might have less of a defensible claim to their credit card statements, social media private communications, and geolocation history. And here you run the risk of losing them altogether, both in terms of cash and data flow, and that is a blow to your financial position as well as your competitive ability. But note that the other side of the coin is damaging as well: By not acting on information you are expected to know, you might look like a very imperfect partner. You might have experienced such a situation yourself, if you have diamond/platinum airline status but still have to enter your personal information. Every. Single. Time.

This captures the personalization paradox: Customers desire personalization and privacy, but personalization requires the reduction of privacy. The answer to this deadlock lies in part in the analogy above: We have to operate within the bounds of a caring relationship. The second part of the answer lies in what I call "soft hyper-personalization." In this approach, you do not make explicit, loud, obvious personalization choices. So, in your digital shoe shop example, you would not greet a customer "Hello, [Name], I see you are in [Location]." Instead, your environment would gently shift to focus on known individual preferences, over-indexing on likely product needs, and using information to change assortment/language/offers. The goal is to create a sense of fit, ease, and functionality at scale. Customers choose you because everything just "works so well," but they do not necessarily realize that each customer is seeing their own version of the service.



your mail behind your back and once showed up uninvited to your parent's house. They know where you are right now and likely where you're going next.

That's probably enough to give a sense of these two relationships; and based on experience, I can guess that we have moved from "Where do I find this magical person?" to "Someone call the police!" But for us, it is important to look

at the details and ask why. The first person stayed within the boundaries of the relationship, likely accruing information little by little and over many interactions where they were expected to learn this information. And all of this was accomplished in the process of providing something of value. The other person, however, completely ignored relational boundaries and norms. They know things that they shouldn't, and they acted on that knowledge. This is the crazy lover/

FIGURE 2 > Key players on the path to hyper-privacy



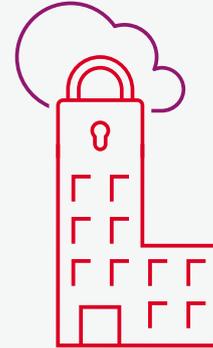
#### Customers

Privacy paradox: want more privacy but keep sharing their data



#### Legislators

Highly motivated with limited success



#### Companies

Implement hyper-privacy for strategic reasons

partner, who should be rightfully feared. Yet, we might allow our brands to become the crazy lover in the pursuit of profit and in fear of missing out – but for how long? In a world where consumers can opt out of the Buff position, a caring relationship is much more promising (see Box 1).

#### Will the hyper-private web become a reality soon?

✗ Thankfully, the hyper-private web will never exist, or it is decades away, right? Well, that depends entirely on three groups: customers, legislators, and companies (see Figure 2). Customers could bring about a hyper-private surface web very quickly by adopting different behaviors and using specific technology. However, individuals seem unwilling to modify their digital behaviors or deploy new tech en masse. Furthermore, we also know that individuals claim to want more privacy but still share information freely when asked, which is called the privacy paradox. So, ghosting will most likely not become a mass-phenomenon too quickly.

The second group, legislators, appear highly motivated to enshrine privacy in regulation. However, their processes are slow, lack technical know-how, and are enforceable only

within their national boundaries: altogether, a poor combination for meaningful change.

That leaves companies themselves as the most likely group to bring about hyper-privacy, and the reasoning behind it is strategic. Large, incumbent companies who already own significant amounts of data and who have established strong customer relationships are exceedingly incentivized to create a hyper-private environment where new challenger brands simply cannot generate valuable data assets easily and cheaply. Small losses of data to incumbents translate into massive losses to challengers, and privacy creates a significant barrier to entry. Anecdotally, significant players like Google, Apple, and Facebook have recently positioned themselves as privacy-first companies, sometimes losing advertising revenue to make it happen, moves that are pro-consumer but also highly profitable.

**Manage customer choice and go for a meaningful “share of data”** ✗ So, it appears that we have a rapidly approaching dark-surface web that is hyper-private and full of ghosts. Marketing managers should therefore expect access to data



to decrease by default. Everyone will need to work with less, both in primary and secondary data sources. And with the lower data availability, the cost of acquiring data from suppliers and partners will increase.

If the Ghost/Buff position is a consumer choice, then companies must worry not only about market share but also their share of meaningful and actionable first-party data. Just imagine that you've lost your CRM data assets, and cannot replace them, but your competitor is somehow intact. How long until they have an overwhelming competitive advantage? To seize the opportunities, companies should take stock of their customer relationships, specify their data needs, and learn what information is critical, advantageous, or irrelevant for their context. They should ensure that their brand is not the "crazy lover" and implement initiatives that drive choice carefully in a trustful relationship, as highlighted in Box 1. The Buff version of service that runs on full information will be more functional than a restricted, less-smart version for Ghosts. The difference in functionality will serve as an incentive for customers to move from Ghost to life-long Buff. ✕

»  
*If there is trust and a  
 worthwhile value exchange,  
 consumers might be willing  
 to share their data.*  
 «



#### FURTHER READING

**Thomaz, F.; Salge, C.; Karahanna, E.; & Hulland, J. (2020):** "Learning from the Dark Web: Leveraging Conversational Agents in the Era of Hyper-Privacy to Enhance Marketing", *Journal of the Academy of Marketing Science*, Vo. 48 (1), 43-63.