IS PRIVACY DEAD in the Digital Age?

and what to do about it.

by Peter Friedman, Chairman & CEO, LiveWorld

Table of Contents

Introduction

Let's face it: Privacy is dead and rigor mortis set in a long time ago—back in the '60s and '70s, when computers began to store our data to target and customize direct marketing. The digital era, internet, and social media have merely brought the embalming to a greater art form. What's more, while the 40-, 50-, 60-year-olds are attempting to put the digital genie back in the internet bottle, the social network generation not only accepts that privacy is gone, they expect it—at least in the sense of personal information as inviolate secret. The truth is that we live in a society where most people prefer to trade their personal information for the goods and services they use in their daily lives.

This is the bottom line: All of us must reconcile with the continuous tracking we face, and also take the responsibility to manage our own personal information. We must usher in a new era—stepping up to better manage our own information, as well as that which comes at us at an ever-increasing velocity. To do so we need new rules and tools to support our efforts.

In Part 1 we'll cover what has happened to privacy in the digital age, how it really works, and how we got here. In Part 2, we'll take a hard but freshly objective look at Facebook—what they really did wrong, what they did right, and what we should expect and demand from them now. Part 3 gets to the solution, based on our decades of managing these issues for some of the largest brands and online communities in the world. We offer a practical, real-world 5-step recipe for how to shape and manage information, personal and otherwise, in the digital age.

Part 1. Life On Blast

To quote New York millennial S.G., "Privacy is dead in this digital age. Everyone puts their life on blast." Don't mistake or water down S.G's meaning. Every element of one's life, good or bad, is out in front of everyone else. Urban Dictionary defines to put someone on blast as meaning to embarrass someone or put them in an awkward position by revealing compromising information.

In this context, any of the millennial generation and those to come demand a level of personalization and socialization that makes privacy as a concept almost laughable. Woe to the brand that doesn't already know everything there is to know about a digital millennial and hasn't pre-tailored the experience based on that knowledge.

How do we reconcile our concerns over privacy and information manipulation by bad actors with the reality of a digital world where the currency of our lives, by definition, is tracked? The advance of digital personalization, socialization and the associated tracking won't be stopped or even slowed down by the current political and business efforts to curtail it. That's the equivalent of trying to stop cars from crashing into each other by going back to horses. What's needed is a new age of responsible personal privacy and information management. This means infrastructure, tools, and rules that enable people to get ahead of the problem, to determine and manage what they share, and to understand and manage the mass of information coming personally to them. Most important, we need to motivate and educate ourselves to actually use the tools to speed up, not slow down, the information revolution.

What's needed is a new age of responsible personal privacy and information management.

One would think with all the headlines, coverage, research, investigations, and even congressional hearings, the substance of the issues, facts, and solutions would be center ring. But as was so profoundly illustrated by the naive, near inept questions put forth by Senators to the CEO of Facebook, the dialogue to date is way off the mark. We've heard lots of hyperbole about invasion of privacy on Facebook, where for the most part, we are talking about tracking the hobbies people are interested in, lifestyle activities, and political comments, all from fairly simple likes and comments. Nevertheless, legitimate concerns exist, especially as related to collecting emails without explicit consent and election manipulation.

"What? You don't already know my preferred music, size, and colors? Everything about me and my friends? You're not prepared to continue the conversation we had 3 days or 3 years ago? I have to click more than once to buy because you failed to keep my data and shopping history? Sooo 20th century. Next."

Whose responsibility is this?

All the drama misses the two enormous elephants in the room: First, almost every aspect of our lives has been tracked, aggregated, trended, and targeted for decades with credit cards, loyalty cards, subscriptions, and more. Second, consumers must take on a much greater ownership of how they handle their personal information and how they personally manage and critically think about all the information coming at them. This challenge began well before social media, and while Facebook has a role in the solution, it is neither the cause of the problem nor the villain some paint it to be. They've made mistakes along the way; it's true they turned a blind eye on the data actions of the third parties they empowered with their platform. Still, Facebook has been at the vanguard of protecting consumer privacy—that is, when it fully rests in their hands.

Facebook is neither the cause of the problem nor the villain.

Ultimately, we the users are our own biggest culprit. We've allowed ourselves to become passive consumers of whatever information social media, cable TV, or any other venue throws at us. Many of us have abandoned critical thinking and active navigation in preference for reinforcement of what we already think and feel by insular digestion of micro-targeted content. To solve the problem, to prevent electoral distortion, to participate in the modern connected world consciously releasing or holding back our personal information, we must put ourselves in the driver's seat, decide where the car is going, and drive it there. Facebook, other companies, and the government can help us with some education, infrastructure, tools, and rules. But ultimately, if we want our personal information protected, if we don't want our minds, hearts, and votes manipulated, we must all step up to a greater responsibility for managing our experience. We can do this through responsible personal Information & privacy management.

Where did this all start?

When and where was the fall of the privacy wall? Do you use a credit card, pay for things, or transfer money from a bank account? Shop in any large physical retail chain or store, buy online, subscribe to anything, visit web sites, download music, watch TV through a cable box or satellite dish, travel with reservations, stay at hotels, fly commercial airlines, buy any kind of ticket to anything, or use your smartphone? Or just have a smartphone in your pocket even if you don't use it? If you do any of these, and no end to other everyday ways we live our lives, you're being tracked, stored, targeted, and re-targeted by the commercial entities that bring you all these goods and services. And that's before you actually registered, filled out information, and answered questions.

That's right; long before Facebook, social media, or even the internet, retailers, banks, hotels, and so on were all collecting and tracking everything they could find out about you—everything you buy, when you bought it, where, what interests you expressed, or researched, or read. Then they used analytics to figure out what your purchases and activities mean about you and what you likely want, and what you likely will do next. Ostensibly they did all this to do a better job of serving you. The more a company knows about you, the better they can make products and services for you, and the more they can tailor their advertising and promotions for you. And of course make more money for themselves along the way.

Then there's the post 911 world of security concern, the Patriot Act, and the NSA monitoring all of our phone calls to store them in a big searchable database. Just as brands want to know more about you so they can predict what you will likely do next and target you for sales and marketing, so our government wants to know more about terrorists and what they likely will do next—so they can target them as well. To do this, they monitor and collect information on all of us. Of course the government says it doesn't look at anybody's private information just because they have it—only at the bad guys' information. Maybe they don't; but they can.

How far does it go?

Have you ever noticed that the ads and coupons in printed materials that come to your mailbox are sometimes a little different than what's in your neighbor's mailbox? (This question is for those older than millennial types who even bother to look in a physical mailbox these days.) Do you ever wonder why that mailbox material is actually of interest to you? How about noticing that the ads you see as you browse the internet, or the ones that appear in your phone apps, cover products you are considering? Are you ever frustrated that Amazon recommends things to you based on a present you bought someone else, but is of no interest to you? That happens because they don't know enough about you to tell the difference. But doubtless you like it when you get alerts on a new book by your favorite author. Welcome to the age of demographic, psychographic, behavioral—and with Facebook—social graphic micro-targeting. It's been going on for decades, and for the most part, we consumers like it, even as we regularly allow ourselves to be oblivious to how it happens.

Ah, but you say, "I only give these companies very limited information about me. They don't know who I am, where I live, and all the other stuff." **Yes, they do!** Or rather, they can. Here's how it works: Companies collect everything they can directly from you as you interact with them—building it out as your digital profile. They get even more if you actually fill out a questionnaire or otherwise answer questions. They note trends and compare everything about you to people with similar profiles to get a better sense of who you are and what you like. But that's not all. They use cookies and pixels to keep track of the internet sites you visit. This information reveals your interests and patterns, data that further builds out their digital profile of you. Then they take the data they've collected and use that to match you into their own customer databases (for example, everything you've ever bought from them with your credit cards and loyalty numbers) and also with third-party massive consumer databases. Companies such as Experian and Acxiom build comprehensive massive databases about all of us, collecting the information through surveys, government publicly available sources, their corporate clients, and buying more from others. An internet company retailer, bank, or media entity just needs two data points about you (say, your real name and email, or your phone number and street address) to match you into those databases with 65%-80% accuracy. That is, you tell the retailer your name and email because you are buying something. If it's a giant retailer and you shop there a lot, they already know all about your shopping habits and can glean information about your family, hobbies, habits, and likely future purposes from just that minimal information.

Then by matching you into the big databases, they can identify a great deal more about who you are, where you live, down to your 9-digit zip code, and a great many things about your daily life. They do all this with the idea of organizing their business and marketing to better target you, deliver messages to you that you will like, and get you to buy stuff and more of it. That's called micro-targeting, and it occurs to the point where the information coming to you will vary from what goes to the person in the house next door, or to the person using the smartphone one hand away. So powerful is this model that a few years

We consumers like it (micro-targeting), even as we regularly allow ourselves to be oblivious to how it happens.

ago **Target was able to figure out who was pregnant from shopping patterns**; they then sent those women brochures and coupons for pregnancy and baby products. The problem was that this was effective even at early stages of the pregnancy and some of those women hadn't told anybody yet. No doubt it felt pretty creepy getting promotional material for something so personal that you hadn't told anyone about yet. Target stopped the promotions; but this is still a good example of the power of common retail analytical practice. Today, some of the largest internet companies are working on predictive analytics. This approach analyzes your current internet behavior to predict future behavior and match ads to it. Now let's apply that to a political campaign. Same idea, but the product is the candidate, proposition, or political view. The message is influence and the purchase currency is your vote.

Let's get friendly with our emotions. When we contact a brand on the phone, Facebook, or Twitter about a problem, and they respond personally—knowing who we are, what we've bought from them, how we use it, the problems we've had in the past, and the history of the specific incident—we like that. Most people love that! That brand is doing a better job taking care of us and our problems. It feels great when they care enough to keep track of our history with them and they go to the effort to make the experience more personalized, personal, and social. This core appreciation in all of us is so strong that brands have built major loyalty programs around it that we just eat up. This has been going on ever since computers enabled micro-targeting and customization of materials in print magazines and direct marketing materials that were postal mailed (circa '60s and '70s). Broadcast TV couldn't target this tightly; but modern cable can vary what you see, cable box by cable box. Because digital technology on the internet can track at a more refined level, it takes the process to an even more micro level. Facebook is the ultimate, so far, because 1) people use it so much every day, 2) users actually participate by liking, sharing, and talking, thus providing massively more specificity to the individual information, and 3) Facebook has done a pretty great job of organizing their service and tools so that they and their advertisers can make use of it.

Critically important and a key driver of the election manipulation is a Facebook advertising feature called dark posts. A dark post is an advertisement seen only by the people the advertiser has micro-targeted. The good aspect of the feature is that it enables an advertiser to better tailor messages to different people. For example, consider a pharmaceutical medicine that's used to treat different diseases. People with disease A are interested only in ad content about its use for disease A. People with disease B want only the ad content about its use for disease B. The advertiser wants to tailor the ad accordingly, as it works better to get the attention of and subsequent purchase by these respective users. The problem comes in when a bad actor, such as an election manipulator, uses the same capability to send conflicting messages (or different kinds of fake news) about a candidate or issue to different people—basically misrepresenting the subject to some or all groups. Dark posts are not widely visible, so the fact that they contain misinformation can easily go missed. In contrast, when a manipulator runs conflicting ads on TV, even targeted cable, or in direct mail, the ads are more visible and the advertisers more likely to be caught by opponents, press, watch-dogs, and/or law enforcement.

So what's the big deal?

A natural question is this: Does anybody care? What's all the noise about if people have been doing this for years? The answer is multifold. On the one hand, people overall don't really pay that much attention to this issue and really don't care that much about it (at least not until it's shoved in front of them with emotional hyperbole). Certainly people have some vague awareness that advertising in direct mail, cable, internet, and social media is tailored to their needs. It's hard to miss that if you've listed photography as an interest, Facebook and Instagram show you no end of camera ads. Or that if you searched for a type of camera at a store website, that same store is sending you ads on Facebook for that specific camera. People have consciously or vaguely traded their information and willingness to get ads in order to get the internet they like for little or no cost. After all, in the last few years we've had actual hacking data breaches of private information that could prove much more damaging than what you like and don't like on Facebook and your email address—such as social security numbers, credit card numbers, bank account information, and purchase histories. Breaches have occurred at companies like TJX, Target, and Equifax. Yet in a fairly short amount of time, all the bruhaha has blown over. Then again, even though such breaches involve information actually considered more sensitive, they don't really feel as personal, or as core to one's day-to-day life, as Facebook interactions. But that's just the point. People value their social media interactions very much—enough to trade their privacy to get it. And no amount of articles, hyperbole, or congressional hearings is going to change that.

People value their social media interactions very much—enough to trade their privacy to get it.

Privacy concern does vary by age. As noted, the social network generation not only accepts this model, but expects the associated personalization. Older generations are more concerned. Still internet and social media usage is pervasive across demographics. So is the tradeoff for one's information. Let's look at some recent statistics from Simmons Research as reported by NBC Meet the Press on April 14, 2018, and by ACP on April 9, 2018.

Large Numbers of people have given up privacy, but they want more control

73%

of Americans use social media with 45% using it 25x/week or more (excluding email use). 43% use online banking.

47%

of Millennials say the information about them online is relatively harmless. Only 30% of baby boomers 55-64 agree with that.

43%

feel once personal information is online - there is nothing you can do about it.

55%

of people believe they understand the risks of providing information online.

63%

would like to have some kind of control.

22%

will use the internet less because of privacy issues.

79%

of US consumers are willing to share persona data for clear personal benefit.

81%

of US consumers feel they have lost control over the way their personal data is collected and used.

These statistics reveal the growing and generational difference in acceptance of a world without privacy. At the same time, most people clearly would like the situation to be different—perhaps not enough to stop using these services, or to force government regulation. But still they'd like to see some changes and have more control—if they can get that without giving up the services. But control isn't really the same as privacy; it's knowing what you've given up and having the ability to tailor it. These are the real questions:

1) How can we give people the depth and range of social media experiences they clearly want, while also giving them more control? And **2) Once they are given more control, will they use it?**

And a very big question, what happened with Facebook that took all this to a new level. That is the subject of Part 2, "The Facebook Dilemma: It's Not What You Think"

Part 2. The Facebook Dilemma: It's Not What You Think

In Part 1, we discussed how privacy has been long dead in the digital age, well before social media existed—and for very good reasons, mostly driven by value for consumers. Still, social media has brought privacy issues in sharp relief, with positive and negative consequences. So just what happened with Facebook and all of our personal information? What was good and bad, and how did it come about? We cover these questions in Part 2 to better understand the problem. In Part 3 we lay out a solution.

Facebook in the vanguard of protecting user information

Facebook being cast as the bad guy is one of the most significant distortions in this story. The social network has been castigated for mishandling users' personal information; but that isn't quite right. Facebook overall has very strongly protected user privacy; but they've made some significant mistakes, which can be corrected going forward.

The dilemma Facebook has faced is how to provide the best user experience, which involves collecting and leveraging lots of data to best understand the user, improve the service, and tailor it to each person, while also managing and protecting that information from abuse. They do this free of monetary charges to the users, in part by creating a great marketing engine for advertisers, which also is reliant on collecting and managing personal data. Advertisers are then able to optimally bring their message and sell their goods to those same users. This challenge

While Facebook generally managed privacy well itself, it left a door open for 3rd party misuse.

isn't easy to accomplish, especially as Facebook manages an ecosystem that's now exploded to over 3 billion users across their portfolio of services.

I can unequivocally state that Facebook's intent for its own actions, and most of its practices, has been to protect user personal information—putting a wall between some of that data and brands. Our company, LiveWorld, on behalf of some of the largest brands in the world—including in retail, consumer packaged goods, pharmaceuticals, and financial services—has worked closely with Facebook for about ten years. One of our clients was Facebook's biggest advertiser, with unlimited direct access to its executive staff and developer team. The company wanted Facebook to modify its policies and provide access to more information about users who came to the brand's Facebook page. Their perspective was that increased access to user information was in the mutual interest of the consumer (better deals), the brand (more sales), and Facebook (more ad revenue). No matter how hard we pushed, Facebook refused as a matter of protecting user privacy—even though it would have meant more revenue for them. For clarity, I'm talking about the information Facebook itself would allow a brand to access directly through its services, not the information a third-party company or brand could access with its own app provided via Facebook. This distinction is where the mistakes started.

Over time Facebook has provided a great deal of targeting information to advertisers. If a user becomes a fan of a brand page, or otherwise interacts with the brand, the brand gets some profile information—but not all. Facebook makes sure the brand doesn't get your email, and quite a bit of other information that would allow the brand to know who you really are. Another example of their determination to maintain privacy is the way Facebook created their custom audiences program. For some businesses, it's very important for them to be able to speak directly to an audience such as their current customers. To accommodate this need, Facebook created a program in which a brand can upload a list of their customers and match them to Facebook users. However, Facebook will not tell the advertiser which users they matched. They tell only the percentage of people they matched.

For an additional layer of privacy, Facebook has volume limits in place, such that they won't match small lists. In some instances, they even have had a third-party company manage the contact list creation so as to create an additional buffer between the brand and the Facebook user information. Clearly these examples demonstrate Facebook's commitment to protecting privacy. The notion that Facebook doesn't care about privacy is simply a bum rap. However, Facebook did make three significant errors on the subject:

Facebook's intent for its own actions has been to protect user personal information

Facebook's Mistakes

To create more value for users, and to spread Facebook's internet footprint, the company enabled third-party applications to run on Facebook. They allowed these third-party apps to collect user information, including emails, without an explicit enough opt-in. When users signed up for these apps, the app collected their Facebook details. Similarly, to build a wider advertising network, Facebook enabled third-party websites to use Facebook's registration system as the mechanism for users to sign up for those sites. Facebook got a great deal of tracking information this way to use for ad targeting, additional advertising space, and research. In return, the websites collected and made use of much of the users' Facebook information. The user got easy access to all these applications and more

Mistake #1

They allowed third-party apps to collect user information, including emails, without an explicit enough opt-in.

The user's Facebook profile information, likes, and other activities were handed over. There may (or may not) have been a check box for users to accept one of those obscure terms of service agreements that nobody ever reads—but not a very clear, explicit check this box to give permission to hand over specific information. Either way, the users were not clearly informed about the information they were sharing and how the third-party company would use it (or sell it). This explains how Cambridge Analytica was able to collect information about users without those users being explicitly aware of it. As part of this muddy opt-in problem, for a while, Facebook allowed those same third parties, once getting you to sign up for their apps, to also access your friends list and collect their information without explicit opt-in. This was a case of the industry being so excited about the intersection of users through social interactions (called the Social Graph) that they ran too fast and missed a fundamental permission requirement. A few years ago Facebook identified this "collect information from friends" problem and changed their API to prevent it without their consent.

Recently it's been reported that Facebook also shared extensive data with device makers (such as Apple, Samsung, and Blackberry) on whose phones people use the service. To Facebook, these are service providers with whom Facebook shares data as a matter of enabling the service to work best for users, and this role thus distinguishes them from third-party applications and websites.

Mistake #2
I promise not to mis-use user data.

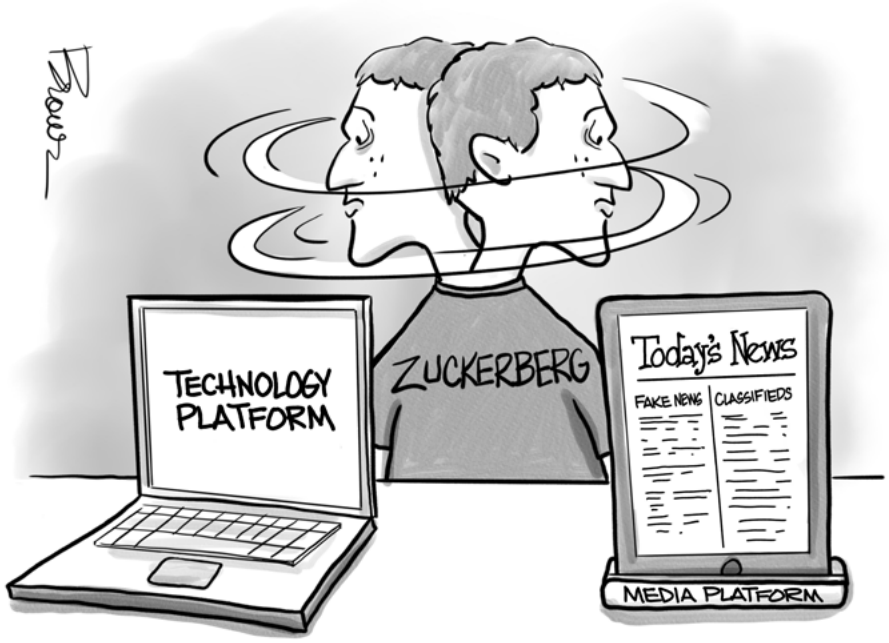
In this light Facebook didn't think it necessary to have users and their friends explicitly grant consent for data sharing with device makers. Nevertheless, the approach did indeed share data without users clearly knowing it, creating yet another issue.

Facebook relied on third parties' word of honor as to whether they were abiding by Facebook's policies—for example, not selling user data to someone else or using it in inappropriate manipulative and perhaps illegal ways. This left the door wide open for all kinds of abuse.

One might ask if Facebook allowing all this didn't make them intentional privacy breakers even if they themselves wouldn't hand over private information? Well no, because at that time the common belief in the world of technology platforms was that managing user privacy was the responsibility of the company or app that was interacting with the user at the time. So the extent to which Facebook proper was the venue, it was Facebook's responsibility to protect privacy. But if it was a third-party company and its app interacting with the user, then it was that company's responsibility. For an analogy, think of personal computers based on Microsoft Windows or Apple Macintosh as platforms and the applications that run on them from tens of thousands of third parties. We expect Microsoft and Apple to protect the private information we hand them as we register the computers. But we don't expect Microsoft and Apple to manage the privacy protection when we register with the third-party applications. We expect the third-party company that makes that application to manage the associated privacy.

Mistake #3

Facebook thought itself a platform, others say media company. It is both and neither.



The third mistake is the really big one. Facebook clung too long to the philosophy, "we're just a technology platform that empowers, but doesn't censor or control, what the third parties or users do." Essentially Facebook turned a blind eye to how their own revolution demands a greater, if different, responsibility role. The technology platform philosophy makes sense coming out of the personal computing age, but not in the world of social media, where applications mix with media publishing and user content, and where the opportunity to collect, manipulate, and abuse information and targeting is much greater. Some say Facebook is actually a media company, with all the editorial control, responsibility, and liability that goes with that. That's not quite right either, because it is indeed a platform that does empower independent third parties and even more so, users to do all kinds of things. Some of those things have good, even extraordinarily positive impact on our lives—and some bad. Neither of which Facebook can entirely control or be held accountable for.

No single entity (Facebook, another company, or government) can control all this without hurting consumers by over-restricting the positive power of the medium. Social media is too large, too extensive, and used in too many ways for regulations alone to solve the problem. Regulations also tend to have negative unintended consequences, including breaking some of the very positive uses of social media.

What should we expect from Facebook?

The problem and the solution rests in that Facebook is neither just a platform nor just a media company. It is a new category that we, for now, can just call a social media ecosystem. It is a mix of platform and media and consumer content usage patterns. This last one is most important. Facebook content, brand content, and media published content all together are a tiny, tiny fraction of the ever-changing user content and behavior on the network. That user content embodies far more information, more personal and social behavior

organized into digital form, than anything that's come before. Think of it as a highway system—not just the highway, but the entire system of lanes, on- and off-ramps, bridges, traffic lights, traffic monitoring and management, the vehicles, and even the people in the vehicles.

Facebook is all these things and more. They should be held responsible for the infrastructure (which they have always accepted). New for them, they are also responsible for the rules and tools of usage, including how laws are managed, and even educating people about them. They have struggled with this responsibility, hesitated, and avoided managing it. But if they take all that responsibility and manage it properly, and still a third party or a user just insists on crashing his car into everybody else or driving off the bridge, we cannot then blame Facebook. In that situation, if Facebook has dutifully set up the infrastructure, tools, and rules to minimize problems, empowered and educated users, and made it easier to catch bad actors, then they've done their job. To date, having popularized this new ecosystem model, Facebook has yet to define and deploy the new forms of responsibility required, although it is starting to do so.

For all this controversy, Facebook isn't going anywhere but up. That's because people like it. Facebook provides consumers with experiences they want. Yes, the number of users is leveling off with slight ups and downs; that's what happens when you hit over 2 billion members (just on the main Facebook service). The key consumer metric is no longer number of users, but the usage per user, active user levels, and users and usage across their multiple platforms (Facebook, Messenger, WhatsApp, Instagram, and more coming). Overall, **these metrics are trending up.** The key business driver is that Facebook has created the most powerful and cost-effective marketing machine in history. This is in part due to the volume of users and usage, in part due to the micro-targeting capability, and in part, the rich set of advertising and communication venues that enable a brand to manage a customer's journey from end to end.

Still, society needs Facebook to step up to the challenges of protecting and managing personal information in this new social media ecosystem model. But how? We'll answer that critical question with real-world practical solutions in Part 3, "New Rules and Tools For Managing Information, Personal and Otherwise, In the Digital Age."

> Facebook is responsible for the infrastructure, rules, tools, and educating people about them.

Part 3. New Rules and Tools For Managing Information, Personal and Otherwise, In the Digital Age

Part 3 works through the solution to the Digital Age's loss of privacy, as explained in Part 1, and directly addresses the real-world dynamics of Facebook and social media as described in Part 2.

Whether driven by Facebook itself or government, clamp-down privacy regulation isn't the answer, as it tends to have negative unintended consequences. For example, in a well-intended effort to protect private information, Facebook has now restricted companies from targeting ads or content to users based on medical conditions and personal characteristics. Sounds good at first, doesn't it? After all, one's medical condition is deeply personal. Except this now means that people with assorted medical conditions no longer get the benefit of treatment information they want and might desperately need. Our social media company, LiveWorld, has clients in healthcare. One of our pharma clients provides a medicine to treat a degenerative muscle disease. The average diagnosis time for this disease is ten years, simply because people don't have the information they need to understand and clearly communicate their problem. Social media is a great way to help people understand the details of their condition, get a diagnosis, and seek treatments. Facebook's well-intended policy to restrict medical information is now a barrier to the needed education and diagnosis—and even to accessing a community of people with the same condition.

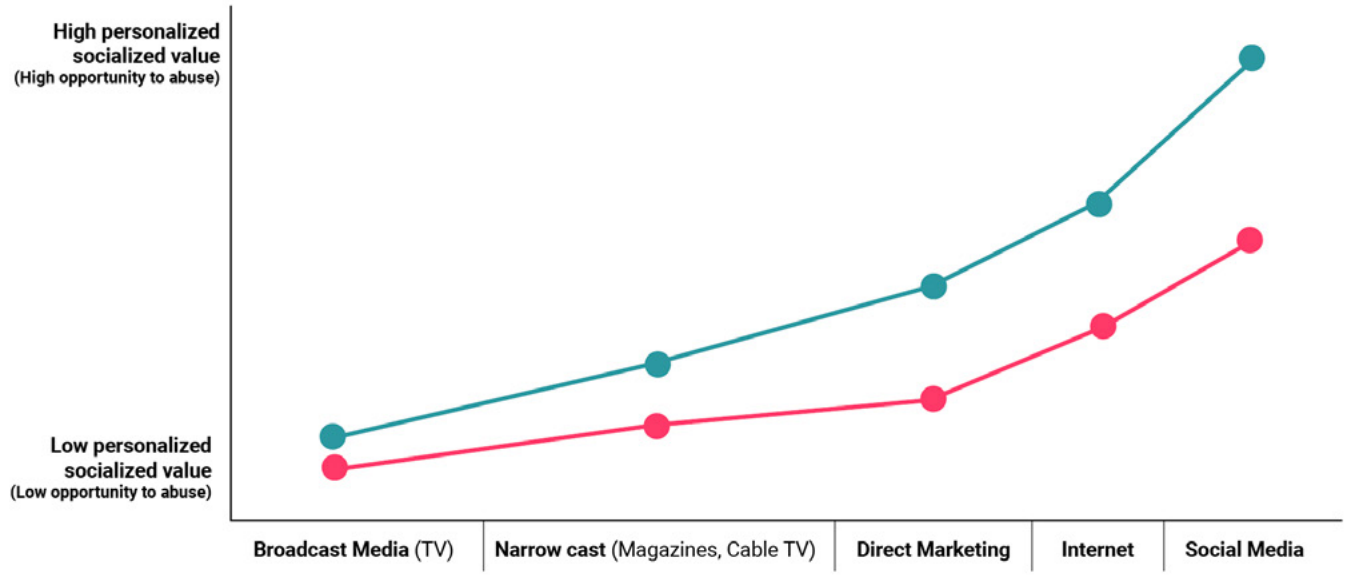
Also well intended to prevent housing discrimination and hate communications, Facebook has removed the ability to target people based on race, religion, and other characteristics. What can be wrong with that? Well, consider people who want more information about their religion—for example, my sister who plans travel to learn more about the history associated with her beliefs. Or African Americans who would be delighted to get information with the nuanced cultural elements of their heritage, so often neglected in general media.

Another well-meaning suggestion has been to remove user data after a period of time (often 2 years or sooner). Is that really in the consumer's interest? Effective customer service requires keeping the customer's history of purchases, issues, and past interactions. Imagine connecting with a car company on social media to discuss a recurring problem that you first reported 3 years ago. The car company says, "Sorry, we'd love to understand this completely, but due to the 2-year content limit policy, we no longer know what we talked to you about 3 years ago." We need ways to collect, keep, and use personal information for positive outcomes while preventing abuse—all with a model that scales.

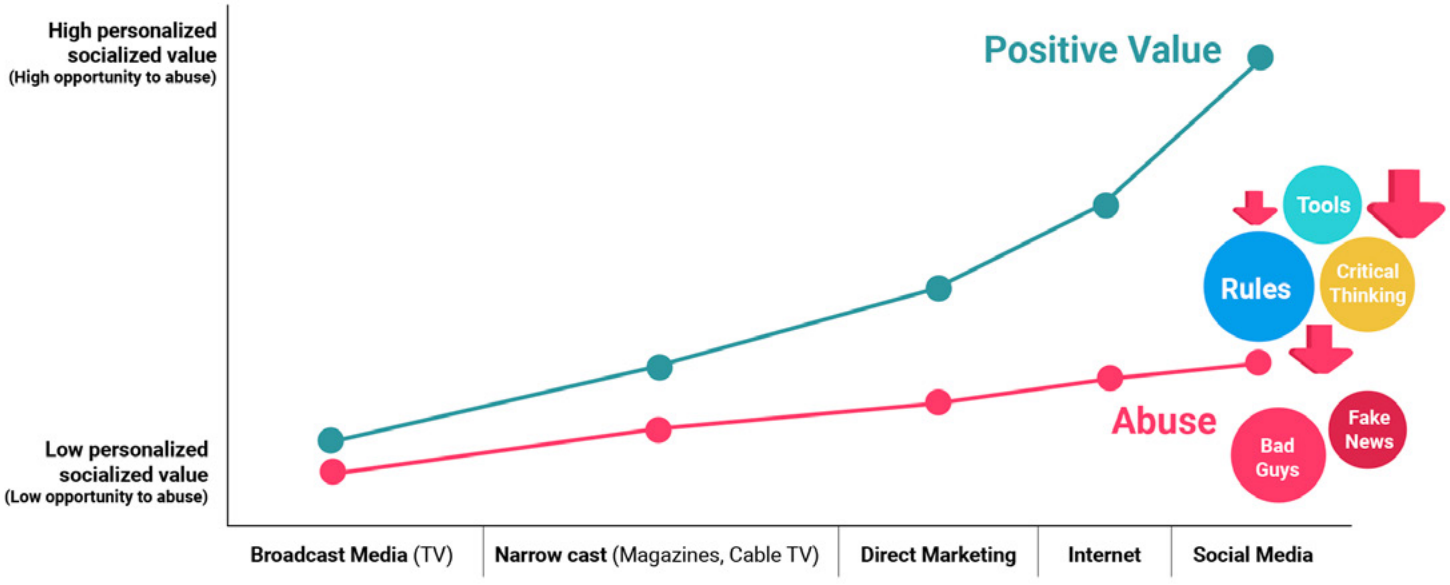
So what's the answer?

The biggest problem is all of us, who passively consume what comes at us, with a decreasing level of critical thinking and questioning. With the right tools, rules, motivation, and education, we can regain some control, enabling us to keep the positive value while limiting the abuse.

The more personalized, social, and involved, the more value you get. But the more micro targeting, the more opportunity for abuse.



Retain the value and push down abuse with the right rules, tools and critical thinking.

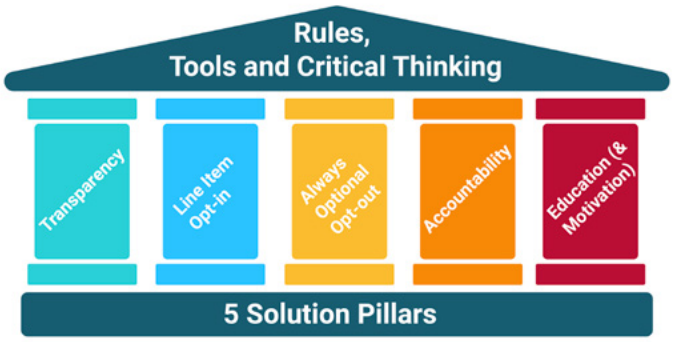


The solution to all this is to support, not curtail, the expansion and use of social media for all its positive benefits. But to put in place tools, rules, and aggressive efforts to motivate and educate our user population to proactively manage the information they share and how it's used. We can divide this effort into two broad categories. The first category is how people can manage all the information coming at them to minimize and stop abuse and manipulation. The second category is how people can be empowered to manage the information that is personal to them. For the latter we could say "how to manage privacy", but this would be a misnomer. It's not about the false notion that one has true privacy anymore—that is, if one intends to be connected. It is a matter of exercising some control on what information you give to whom and what happens to it on an ongoing basis.

The solution to all this is to support, not curtail, the expansion and use of social media for all its positive benefits

A five-part solution

Five pillars form the solution: Transparency, Line-item Opt-in, Always Optional Opt-out, Accountability, and Education. The industry, in particular Facebook and Google, are taking steps on these. But they, the government, and we as users all need to do more.



I. Transparency

Transparency is key to managing the velocity and range of data coming at us, such that we are not subjected to the false information, manipulation, and other abuses of the past few years. Or at least we have the context with which to manage and mitigate it. Transparency means knowing from whom and where the information we see is coming and what other information that source is presenting to whom. Put simply, if we know who is targeting ads and content and what else they are up to, then we are better able to figure out their motives and accuracy. This is not unlike the way television and print ads have been regulated for many years, requiring disclosure of who paid for the ad. At least then when an ad is broadcast on TV, many people see it, including opposition groups and law enforcement, who can call out false information. Because social media can target ads to individuals without anyone else seeing them, transparency is all the more important.

If we know who is targeting ads and content, then we are better able to figure out their motives and accuracy.

Google has taken **a good first step** regarding political ads. They'll require all political election advertisers to prove who they are—providing a government issued ID and other information. Google will release a Transparency Report specifically describing who is buying such ads and how much money is being spent. Further, they will build a searchable library of election ads, such that anyone can find the ads and who paid for them.

On the advertising front, Facebook supports and is implementing the principles of the **Honest Ads Act** (see detail below). Further it's releasing **new tools and policies**, such as showing not just an ad's content, but how many people saw the ad, how much money was spent on it, and broad demographics about the ad's audience. Another tool called **"View Ads"** allows any Facebook user to see a slate of ads that a page is running at that moment—plus tools to allow researchers to delve deeper into what's going on, though it appears to lack features to search across ads.

Facebook is also taking these steps to reduce distribution of false news (Source: Facebook):

- Independent third-party fact checkers may review news stories. Stories rated false will be placed lower in News Feeds. Pages that repeatedly share false news will get even lower distribution, and their ability to monetize and advertise will be removed.
- If third-party fact checkers write articles providing more information on a story, those will be presented to users right below the offending story.
- People who share stories rated by the fact checkers as false will be notified they are spreading false information.

The Honest Ads Act proposed in the US Congress attempts to address some of these issues as well. If passed, this law will require large digital platforms (50 Million unique visitors or more a month) to maintain complete records of advertisers who have spent more than $500 on ads during the previous year. The records must also include the ad rate, name of the candidate or office supported, and contact information of the ad's purchaser. The bill requires the platforms to make reasonable efforts to ensure foreign nationals don't buy ads that attempt to influence elections. The law essentially expands the definition of the 46-year-old Federal Election Campaign Act's defamation of "public communication" to include paid internet or digital messages.

Source: https://www.cbsnews.com/news/facebook-hearings-what-is-the-honest-ads-act/

While these are all good actions, they do not address how easily and powerfully social media can pretty much let anybody advertise targeted messages to anyone. It will be hard to screen what is an election ad, and what nation it's coming from. Applying the law just to platforms with over 50 million unique visitors and over $500 ad budgets, misses the reality that a bad actor can be effective by working across multiple smaller platforms and with separate below $500 budgets that together can add up. Further even a few hundred dollars can be very effective in social media. Having a report after the fact doesn't help users make judgements in the real-time high-speed digital world. Google's searchable database is a very good idea, but it too misses the need if it's only after the fact or if users have to go looking for it. Facebook enabling people to report what they think is false news is a great step, as it leverages the power of 2 billion+ users.

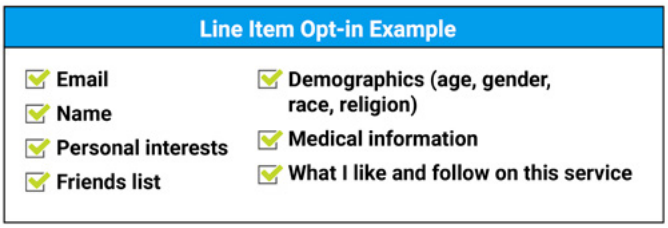
But all of these stop short of fully empowering users to know what they are looking at and creating a structural context to evaluate it better, and then holding bad actors accountable. The needed solutions can be done with some rigorous actions that won't cost much but will go very far. These need to be designed so that any everyday user can drill down and across to figure out what's going on and make critical judgements. It's not enough to enable just researchers and professionals to study the matter. Every advertiser (not just elections or political) and every news/information publisher, of any size, on a platform of any size, needs to prove who

they are, with a government ID and a bank account or credit card information. Each has to have a registered page of some kind on the platform. There must be just one master page for each entity, though they can have additional linked pages for specific products and themes, as long as those are all visibly and obvious linked to the master page. All this so we can really tell who's behind these ads and what they are really up to.

Every ad and every piece of published content has to have an obvious icon and link back to the registered page of its producer. This makes it possible for a user to drill through with one click to see where an ad comes from. Additionally both current and the entire history of ads and content from that advertiser or publisher has to be listed on the registered page or a linked to page on platform-hosted (e.g., Facebook). This way a user can also see what else a given advertiser is saying to other people and the history behind it. This information will help curtail the abuse in which a political candidate takes one position or attack with one set of voters and an opposite, conflicting position with other voters. Last there should be links to see what third-party fact checkers have to say about it, their articles, and also any user ratings of the accuracy of the content. All of this information should immediately be available in real time updated searchable databases (a la Google's idea) but available to users as well as researchers. With this model, just as with television ads, everything can be seen by the opposition and by government agencies responsible for managing and ensuring compliance with election laws, commercial advertising laws, and regulations relating to fair and balanced news.

II. Line-item Opt-in

Social networks, websites, apps, and device makers have the right to require your data for you to use their services. The network just has to be clear about it. The users have to have the right to walk away with their data at any time. Under the new European Union GDPR (Global Data Protection Rules), providers have to give users an explicit point of opt-in before collecting their information. This is the right idea but given the depth of what can be collected and the user propensity to skip reading the terms of service, we need more than that. There should be an explicit Line-item Opt-in. That is, there should be an explicit checkbox for each type of information a user is allowing to be collected. For example, a box should be required for each of name, email address, age, gender, race, religion, medical conditions, interests, conversations, and so on. This way, users consciously decide what they are willing to turn over. Following on examples above about how over-clamping down can have unintended negative consequences, the Line-item Opt-in empowers the diabetes patient to allow medical content to be collected and in turn get relevant coaching, treatment, and medication content.



Some companies, such as Apple, are already taking steps to empower users with Opt-In capability by preventing companies from automatically tracking them—another good step. But if history is an indicator, most people won't make use of these features. After all, users can turn off or delete the history of cookies in their web browsers, but few do. This is partly because they want the value that results from giving up their information, and partly because they tend not to pay attention to such features anyway. This reality of user behavior further underscores the need for the explicit line-Item opt-In model.

III. Always Optional Opt-out

While GDPR is not a regulation in all countries, it has a great concept that is included in the pillars detailed here. It requires service providers to provide the user all the information they have about that user if the user asks for it. GDPR also requires a service provider to offer an Opt-out, sometimes referred to as delete everything you have on me, or a right to be forgotten. All these are good requirements. But again, just having this is not explicit enough. People simply forget what they have signed on for; as such, there should be not just a mechanism to opt out, but one that is explicitly always available. To ensure this, the rules should be that the service provider has to provide an annual opt-in renewal to users, unless the user explicitly agrees to automatic renewal and gets an annual reminder that they've done so. By taking this approach, not only do we ensure the users know about their opt-in, but we avoid government or the services mandating a time limit on keeping data, such as the 2-year limit. As

described earlier, such time limits have the unintended negative consequence of diminishing the value the services and companies can bring that users very much want.

IV. Accountability

Here's where rules, policies, and government come into play. The social networks and platforms must create the tools and set up the policies as we've described. They must also empower their users to help monitor for abuse and provide them ways of easily reporting it. Then the social networks have to be accountable for reviewing such reports and escalating illegal activity to government agencies. Just as the pharmaceutical industry has to watch for drug adverse events and report them to the FDA. Pharma companies do this every day in social media to manage their regulations. So can the social networks can as well step up, monitor, and report abuses on their own systems.

We don't want the government to specifically regulate what a company can collect or how long it can keep it, or whom it can target. This leads to negative unintended consequences. However, the government should require the social networks to have the proper transparency, tools, and policies, including monitoring and reporting illegal actions by third parties and users. For example, let's take the scenario where two companies are targeting advertising based on race or ethnicity. The first one is providing culturally relevant information to African Americans that they very much want. The second one is using the micro-targeting to practice housing discrimination, essentially keeping their ads and offers away from a minority group. The answer is not to take the targeting capability away and thus lose the benefits of the first case, but to better monitor abuses such as in the second case. Algorithms can easily track any use of race or religion for ad targeting and serve them up for human agents to review. Human agents can determine if the ads are essentially supportive of the interests of the users or discriminatory or hateful. In these abuse cases, the advertisers can be reported to legal authorities for prosecution. At its core, this is no different than reporting and prosecuting any such discrimination in advertising and business practices be that magazines, direct mail or even in person sales. We just have to understand that on social media, it is easier to target improperly, but it is also easier to catch and prosecute if we have the right rules and tools to do so.

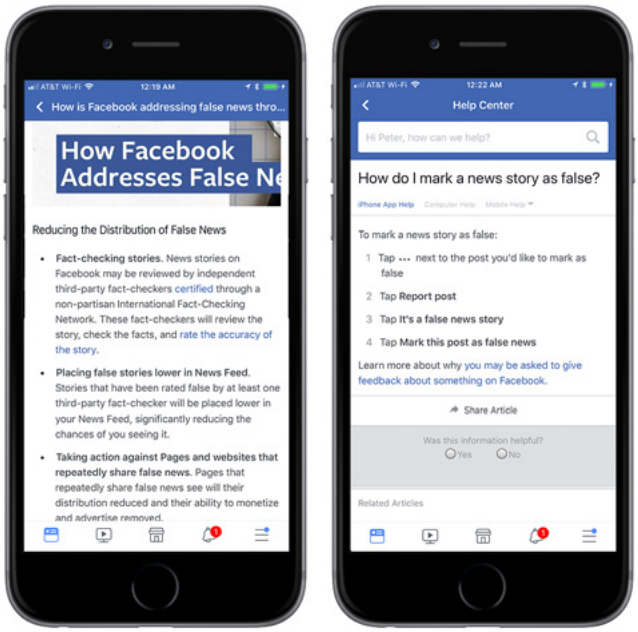
Accountability isn't just a matter of regulating the social networks and advertisers. Our society of users has to step up and take accountability as well. Ultimately the most important and most critical need is for us, all of us who use these services, to go beyond just passively receiving information and believing it, to leveraging the power of these platforms to better review, question, understand, and make judgements about the information. This applies to both the information we receive and the information we hand over about ourselves. We have to recognize the reality, power, and value of the digital and social media revolution. That we have already gone beyond the past world of isolation and arcane notions of privacy, some of which never really existed. That our connected lives bring us more and give us more opportunity to be individuals, and at the same time be part of something greater through dialogue and relationships. As the users of these services we can't just passively hand over our information or passively believe whatever is thrown at us. Each of us has to take charge if what's happening to and around us.

Our society of users has to step up and take accountability.

First, we have to take control of our own information and be in charge of what happens to it—not in the name of privacy, but to drive the benefit of its use and prevent mis-use. Second, we have to actually watch for and report abuse, leveraging the new tools provided by the social networks. Third we have to actually think about the information coming at us—critically think about, review, understand, and make judgements about that information. We need to drill down and across the medium to evaluate the information, its source, and alternate views.

V. Education (And Motivation)

Our taking accountability demands not only believing in this approach, but also educating ourselves, and especially our children, with the knowledge and skills to do so. In the home, it has to be considered as important and as serious as teaching our children basic social skills, how to talk, behave, and interact with others. Keep in mind that they live in this world



the moment you let them touch an iPhone or iPad, and the day they go out to even the earliest of child care. We can proactively see to their learning or let them find out on their own.

In schools this means federal, state, and local required curriculum for critical thinking, personal information management, and high velocity content review and navigation in the digital social age. The social networks can and must help by creating education and training materials. Today Facebook is publishing articles on its own site about how to spot false news and providing venues for people to provide feedback when they think stories are false.

Facebook's attempt to educate people is helpful, but doesn't go far enough.

This is a good step, but neither comprehensive nor proactive enough. Essentially it's like saying, "we've created useful limited reference material for the very few of you who will bother to look at it." Rather we need effective, multi-media, constantly updated training materials tailored to all ages from pre-school to seniors. The platforms, as a matter of doing business, should create these. But with or without them, we need this as core curriculum for our society.

Every action by the social networks, every government regulation, and every recommendation we are making will go nowhere if as a society we don't hold ourselves accountable for stepping up as well with education, motivation, and fundamental acceptance of responsibility for the experience we have.

Yes, in the digital age, privacy is dead and has been for many years. But we can move beyond that to better lives by ushering in an era of proactive and responsible management of the personal information we give and the non-stop information we receive.

About The Author

Author: Peter Friedman, Founder Chairman & CEO, LiveWorld
www.liveworld.com | Twitter: @peterfriedman | Instagram: peterfriedman

Peter Friedman is a social media visionary and veteran with over 34 years experience in the space (22 at LiveWorld, Inc. and 12 at Apple). He's provided multiple global brands with strategic social media guidance and delivered hundreds of social media programs for them in multiple countries and languages.

Peter founded LiveWorld, raised over $100 Million in private rounds and an IPO, grew the company to hundreds of employees, and managed its downsizing, survival, and re-invention through multiple market crashes, recessions, and resurgences. He is a fine art photographer, celebrated public speaker, and author of the book, "The CMO's Social Media Handbook, A Step By Step Guide For Leading Marketing Teams in the Social Media World." He holds a bachelor's degree in American History from Brown University, and an MBA from The Harvard Business School.

Peter's life-long mission is to help people create more value together, through collaborative relationships, than they can alone. Connect with him @PeterFriedman on Twitter.

Disclosure: Peter's 401K holds stock in each of Facebook and Apple.

About LiveWorld

LiveWorld provides enterprise-class software and services for managing customer conversations in social media and messaging apps, on the web and mobile devices. By blending human engagement and automation, we help companies get closer to their customers to bolster relationships, loyalty, and lifetime value. Our clients include Bank of America, Pfizer, Wells Fargo, and Zoetis, among others. Visit www.liveworld.com to learn more or contact us at @LiveWorld.

Learn more at **www.liveworld.com**.