Beware of digital zombies: How to manage the threats posed by your online activity

Ongoing research on digital zombies — old online activities that come back to haunt us — demands that we rethink the nature of privacy.

September 1, 2024

When U.S. comedian Kevin Hart was offered a gig hosting the 2019 Academy Awards, probably the last thing on his mind were his Twitter (now X) posts from a decade ago. But it

didn’t take long for internet sleuths to dig up a series of homophobic jokes he had shared online. Ultimately, those old tweets ruined his chances of hosting the Oscars.

This is an example of a digital zombie, which involves content posted long ago, often for a specific audience, in a specific context, or simply at a time when the content wasn’t considered problematic; but it resurfaces later, causing trouble for the content creator.

A new working paper by IESE’s Tawfiq Alashoor — co-authored with Mazen Shawosh (King Fahd University), Nicholas Berente (University of Notre Dame) and Thomas Grisold (University of St. Gallen) — looks at what can happen when digital zombies are resurrected, coming back to haunt the user in the form of ruined reputations, legal issues and threats to personal safety.

The 5 stages of a digital zombie

The authors chart the lifecycle of a digital zombie in five stages:

1. **Birth.** The moment you post anything online, you’re creating a digital trace — some form of content that contains a timestamp and is tied to a certain context. Even your scrolling habits are leaving remnants of your psychographic profile for all time.
2. **Dormancy.** These traces can lie dormant for months or years, as the legal and social context — the general zeitgeist — shifts.
3. **Resurrection.** Once the context shifts, these digital traces may surface, such as when other users actively search through the online history of a user. A revived dormant post may take on a life of its own. When this happens, the digital trace has morphed into a digital zombie.
4. **Post-resurrection.** This is when the original creator of digital traces acts retrospectively to manage or mismanage the revival in some way.
5. **Death.** This is when some impact occurs, such as a job loss, as in the case of Kevin Hart.

It is important to note that any initial impact may not be the final outcome. Reaction to zombies may deescalate and the public could forget about the zombie. Zombies can slink back to their graves. This happened with movie director James Gunn, who was fired by Disney for his digital zombie but later rehired after the initial outcry had died down.

No skeletons in your closet? Think again

Although the authors use case studies of three high-profile media personalities (Kevin Hart, James Gunn and Alexi McCammond), they are keen to broaden the discussion beyond these headline-grabbing examples. A digital zombie is not necessarily tied to homophobic, racist, sexist or hate speech online; it can emerge based on much more subtle content that might even appear harmless to the user.

Even “safe” opinions can become liabilities. The Arab Spring is a dramatic example of how “acceptable” can become “unacceptable” as the time and context shift. Social media posts made by anti-government protestors in a spirit of hope for change later landed users in hot water, including prison, as the pro-democracy movement fizzled out.

When it comes to digital privacy, most people are careful not to post their phone number or home address online — yet they then proceed to share all kinds of personal opinions in public forums. Oversharing is so baked into social media that few consider the evolving nature of privacy today: It’s more than safeguarding personal data; we need to appreciate how privacy is context-and-time dependent, and how phenomena like digital zombies are part of a growing challenge with unforeseen and unintended downstream consequences.

Each one of us leaves all kinds of digital traces, from the stories we’ve scrolled to the videos we’ve watched, and for how long. And as a previous Facebook study has shown, users’ personal attributes, including their religious and political affiliations, can be accurately predicted based on just 10 likes. Users rarely consider what kind of psychographic profile they’re generating through their daily online activity.

With shifts in context and time, these digital traces get reframed — and that’s what we’re unprepared for. Even privacy laws, such as Europe’s General Data Protection Regulation (GDPR), are inadequate to prevent this. Such regulations take a long time to create and implement, and what protects you today may not be fit-for-purpose tomorrow. Even the “right to be forgotten” (allowing a person to have their personal data erased) cannot protect data from being screenshotted or archived in the Wayback Machine.

Managers need better tools to vanquish digital

zombies

It’s not just individuals who bear the costs; organizations face reputational risks as well. Digital zombies can jeopardize celebrity endorsements or CEO appointments, putting projects, products and events on hold, and ultimately impacting the bottom line. The typical management strategies employed in such circumstances aren’t enough to vanquish digital zombies:

- **Ignore.** While simply ignoring the outcry might work, because public attention spans are short, this approach can also backfire. Silence may be interpreted as support, helping to feed the zombie.
- **Negate.** Eliminating the post and providing a credible explanation of the original context can help. James Gunn saw the rise of a countermovement defending him that led to his eventual reinstatement. That said, counterarguments can sometimes help keep the zombie limping along.
- **Align and apologize.** Admitting the error and apologizing is a simple and reasonable approach. But sometimes it’s not enough either, as the journalist Alexi McCammond discovered. After apologizing, she ultimately resigned from her appointment as editor of *Teen Vogue*.

Where there is danger, there is also opportunity

The limitations of these strategies highlight the urgent need for more comprehensive approaches to data governance and privacy management, not just for individuals and organizations, but for society as a whole. The authors join calls for “a contextually sensitive and temporally attuned understanding of privacy decision-making in the digital age.”

Namely, they believe we need to stop treating digital traces as neutral, and conceive of them and their implications within their broader societal context, linked to values and norms specific to certain social, political and historical events and periods.

How might such a conception change the way we treat data?

For one thing, social media platforms are designed to display posts chronologically, with old posts fading from current view as the timeline progresses. This format makes it easier for old traces to accumulate in a “digital grave.” Rather than operating under the presumption of

“out of sight, out of mind,” platforms should provide users with easily accessible ways to remain conscious of old digital traces so they can delete or manage them efficiently.

Given the unpredictable nature of digital traces — not knowing which ones will one day give rise to a digital zombie — this requires platform designers and creators to get better at foreseeing potential harms and building remedies into their choice architectures for users.

It also requires users to appreciate the reality of digital zombies and the five stages they pass through, and remain highly attuned to societal shifts, so they can be prepared to manage any consequences in a well-thought-out manner.

There is already an emerging market for advanced privacy management solution providers. Companies such as ReputationDefender and BrandYourself offer services to mitigate the harm caused by digital zombies through suppressing negative information, promoting positive content and offering digital privacy guidance.

Browsers also have a role to play. Search engines that reduce data collection and sharing with advertisers, like Brave, set a standard for privacy, pressuring others to follow suit. There is plenty of scope for the IT industry to transform the problem of digital zombies into opportunities for innovation.

Ultimately, significant shifts in how people manage their privacy may only occur when personal data is perceived as having tangible monetary value — essentially, when privacy becomes something that pays.

This aligns with emerging trends in data privacy, where users are starting to demand greater transparency and control over how their data is used. If people have a stake in managing their data, there may be a stronger incentive to engage in safeguarding it proactively.

At a glance:

READ ALSO: The contexts putting your privacy at risk

https://www.youtube.com/embed/pzLhk440A1A?list=PLu80P54BN4lMS5tT0QbsEq9se310t5D5

L

https://cfvod.kaltura.com/pd/p/1766931/sp/176693100/serveFlavor/entryId/1_es71mkl7/v/1/flavorId/1_9u0ds5pd/name/a.mp4

https://www.youtube.com/embed/0zOH30t_8Tw

Tawfiq Alashoor

Assistant professor in the Department of Operations, Information & Technology at IESE. His research focuses on privacy and cybersecurity decision-making in emerging AI-supported technologies, including apps, conversational agents and robots.