EXISTENTIAL CRISIS

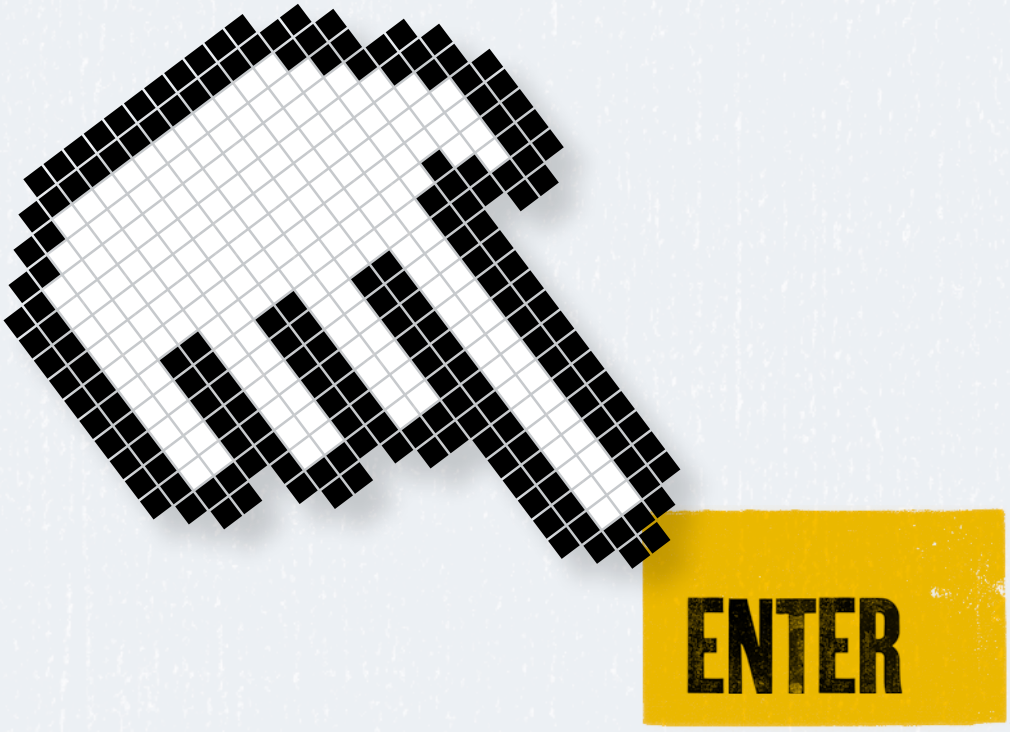
Welcome to the world of data permanence, where digital information will live forever, says Brunswick's PHIL RIGGINS

"No man's correspondence is safe. No man's confidence can be deemed secure; the secrets of no family, of no individual, can be guaranteed from reaching the ear of a Cabinet Minister."

You could be forgiven for thinking this quote was ripped from the pages of last week's *Financial Times* or *The Economist*. Secrecy and government surveillance of digital communication are currently hot topics. But in fact, the quote appeared in *The Times* in 1844, related to what was then described as the "Post Office scandal," when *The Times* railed against the British government's eavesdropping on the correspondence of Italian republican and unification activist, Giuseppe Mazzini. At the request of its Austrian allies, the British government did what many allies might do if asked today: it opened Mazzini's mail and shared it with the Austrians. The more things change, the more they stay the same.

Before the internet and smartphones, all you needed was a match to burn that incriminating letter or note – gone in a puff of smoke. Forever. Or skip the note and share secrets in meetings on a park bench or lonely beach. The technology was simple, even romantic.

Today, most of us have no idea how our communications devices and their networks really work when handling our data. Send and delete email, empty deleted email folder – job done. Only recently has awareness grown of "data permanence," the concept that all of our emails, text messages, tweets, Facebook posts, data sitting in the cloud – you name it, all of our digital information and communication basically lives forever, always discoverable in some fashion. If it ever emerges in a government data trawl →

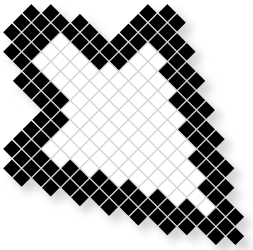


or hacker break-in, such information can potentially destroy a career, damage a business's reputation or lead to very large government fines.

The Sony data hack in late 2014 opened a trove of embarrassing personal emails to global media exposure, scuttled the world premiere of Sony's Christmas movie *The Interview*, and prompted the US and North Korea to consider cyberwar plans. And that's just one recent example of the impact data permanence can have.

Do a Google search for "Libor rate rigging" and you will see how easy it was for government investigators to discover, years after the fact, cringe-worthy and incriminating banter between bank employees across several major institutions entrusted to set key interest rates for the world's financial markets through the interbank lending rate, or Libor. Chat-room conversations and emails became evidence that brokers rigged the system for their own profit. The scandal has cost several financial institutions around $10 billion in fines and sullied corporate reputations. All an investigator needs are forensic data tools and a bit of time to explore the internet or a company's server, and the hunt is on.

The new reality for communicators is that anything stored digitally may somehow, someday, become part of a public conversation. Digital is forever, and private data can become very public. This has profound implications for all of us. Not only do we have to accept the possibility of total transparency, we also have to understand that once we hit "send," the information lives on.



Data permanence just is. It exists – and we have to learn to live with it

Yes, we can delete that ill-advised drunken tweet immediately after our blood runs cold with the realization of what we've done. But it may have already been retweeted or screen-grabbed. Just ask Congressman Anthony Weiner, whose political career was self-torpedoed when he accidentally tweeted to his many followers what was meant to be a direct message containing intimate photos of himself to one woman (not his wife).

To make matters worse, it doesn't even have to be our own email that brings our world crashing down. US four-star General David Petraeus, the former CIA Director and military legend who was once thought of as a possible US presidential candidate, had his career derailed indirectly by his biographer/mistress Paula Broadwell's emails to another woman threatening her and telling her to stay away from the General. The subsequent FBI investigation into the harassing emails proved personally uncomfortable and professionally destructive.

But isn't there an app for that? A technological patch like the ones that calmed our fears about "Y2K"? Isn't someone out there working on a software program of such military strength that it will allow us to override this vulnerability and return to a comfortable world where private data is private?

Yes, people are working on it. There are books, consultancy specialists and products such as "digital shredders" that obliterate unwanted information. But while there is plenty of innovative thinking, such efforts will probably never be enough to allow us to retreat into blissful ignorance. Data permanence is no Y2K.

No matter what solution is put in place, it will necessarily involve human beings and therefore be prone to failure. The human brain may be the most complex computer ever devised, but historically our ability to control what we say or do is very poor.

The digital age demands a different type of corporate culture from any we have known, a culture that understands how reputations can easily be destroyed by disconnects between public personae and "private" communications, between what a company claims to be and what its communications actually demonstrate.

Is data permanence a good or a bad thing? The answer, of course, is both. Good, in that it should help keep companies and people honest. Bad, in that it leads to self-censorship and less appetite for reasonable business risks. But such a question also misses the point. Like an old MySpace page that won't die, data permanence just is. It exists – and we have to learn to live with it.

PHIL RIGGINS is a Partner in Brunswick's London office and co-leads Brunswick Insight, the firm's research and consulting arm.

KEEP YOUR HOUSE IN ORDER

Your digital past could come back to haunt you. Be ready by following these steps:

1. Upgrade your culture
Assume total transparency and remember that no technological fix is ever foolproof. Understand that every byte of information within your business and under the control of your employees could be made public. This should influence your entire company's behavior.

2. Be clear about the risks
Any sensitive email could wind up in a story on *The Daily Beast*. A bit of self-awareness and honesty can help avoid disasters. That isn't to say you should lead a boring life, just keep your eyes wide open to the risks.

3. Prepare for the worst
Have a contingency plan and be prepared to use it.

4. Upgrade your systems
Protect against intruders who want to steal your confidential and valuable information by ensuring data protection systems are robust and up to date.