THE BLOG 12/15/2014 02:46 pm ET | Updated Feb 14, 2015

Sony 'R' Us

By Marty Kaplan

The most shocking thing about the digital disemboweling of Sony Pictures' computer data is that anyone would actually find it shocking.

That goes for everything from the vulnerability of everyone's personal and proprietary data, not just Sony's, to the revelation that a sausage-making industry like the movie and TV business is likely to be run by people who know their way around an abattoir.

If you haven't been following the Sony story, the gist of it is the malicious Nov. 24 public dump of 40 gigabytes of private email, employee evaluations, complaints, salaries, medical records, passwords, social security numbers, movies, scripts, PowerPoint presentations, financial spreadsheets, executive suite gossip, marital confidences, temper tantrums, profanity, flattery, deceit, contempt, obsequiousness, insecurity, bad taste and (in the view of at least some people) evidence of racism, sexism and a host of other indefensible behaviors.

As of this writing, the culprit most widely suspected of breaking into Sony's servers, stealing its intellectual property, violating its trade secrets, invading its employees' privacy and doing their best to humiliate the company and damage its business is the North Korean government, posing as a group calling itself Guardians of Peace. The motive: revenge for *The Interview*, a Sony Christmas comedy about assassinating North Korea's leader, Kim Jong-un. An alternative theory is that the perps are fiendishly talented malware coders with a score to settle with Sony for reasons ranging from its efforts to crack down on piracy to allegations of arrogance and greed. Whoever is responsible, their message to management is that the carnage is far from over.

If you've paid any attention to the files that former NSA contractor Edward Snowden turned over to journalist Glenn Greenwald, you know how invasive and pervasive U.S. government surveillance has become. Whether you believe that such spying is legal and justified by the threat of terrorism, or that it's unconstitutional and corrosive of the very democracy that terrorists threaten, what's inescapable is the scary likelihood that privacy, secrecy and security are technological illusions. There is a ferocious battle going on today between white hat hackers and black hat hackers, and though one or the other of those camps may momentarily outfox the other, the chances that any data — government, corporate, or personal — can be reliably protected from prying eyes are close to nil.

How should that make us feel, let alone behave? A few years ago, when the TSA introduced body-scanning technology at airports, there was an uproar about its potential for abuse — the fear that contractors were casting us as unwitting performers in some kind of pornographic security theater. No, no, came the reassurances. The scans can't be stored. The faces will be pixilated. The genitals will be blurred. Your picture will be seen in a distant room, with no possibility of recording it or connecting your identity to your image. It turns out, of course, that those images provided plenty of entertainment for the staff. As one former TSA agent confessed to Politico, "All the old, crass stereotypes about race and genitalia size thrived on our secure government radio channels."

It would not be farfetched to assume a comparable nakedness of our emails and texts, our photos and finances, our locations and contact lists, our browsing and phone calls. There has been much public discussion about what privacy rights we should have online, what terms-of-service transparency a social media, e-commerce or any other site must provide. But I can't help thinking that all the privacy policies in the world won't be able to prevent a determined tyrant, crook, sociopath or teenager from making the Sony data dump a demoralizingly common occurrence. And looming beyond that industrial crime, of course, is a far darker digital terrorism capable of bringing down power grids, financial markets, transportation systems and military defenses — the "cyber-Pearl Harbor" that Defense Secretary Leon Panetta warned about two years ago.

Much has been written — much of it erroneously — about people's attitudes toward privacy in the digital age. Facebook founder Mark Zuckerberg has been misquoted as saying that young people no longer care about the norm of privacy the way previous generations did. What polls actually show is that Americans under 30 are substantially less likely than those over 30 to agree that it's "more important for the federal government to investigate possible terrorist threats, even if that intrudes on personal privacy."

The Sony hack threatens to take the debate between civil liberties and national security, between freedom and privacy, out of our hands. The Guardians of Peace, or whoever these or the next vigilantes are, couldn't care less about social contracts. Their tech prowess alone could engineer a bloodless revolution, the transformation of any society into North Korea, where fear rules communication and no one dares risk an honest idea about anything. It's not that much of a big deal when hackers out producer Scott Rudin for dissing Angelina Jolie as a brat. Yes, it's infuriating when the financial and medical confidentiality of thousands of Sony employees is violated by cyberthugs. But what's most sobering is that the plausible nightmare of having our private words exposed will drive our democratic society to pre-emptive self-censorship, hustling us, without a shot being fired, toward the tyranny of Pyongyang.

This is a crosspost of my column in the Jewish Journal, where you can reach me at martyk@jewishjournal.com.

Follow Marty Kaplan on Twitter: www.twitter.com/martykaplan

Marty Kaplan
USC Annenberg professor and Norman Lear Center director