Computing Technology and Survivable Journalism

Hal Berghel, *University of Nevada, Las Vegas*

Ironically, the very technology that the media pundits suggest might get journalism out of the hole might actually be making the hole deeper.

Ex-journalist Annalee Newitz's talk at the 27th Chaos Communication Congress (27C3) in 2010 conveyed the "received view" of modern journalism: recent technology advances are rendering traditional print-media-based journalism impotent and, as a consequence, future jobs in journalism will require increased IT skills (www.youtube.com/watch?v=6gBtLER9C70).

No news there. But Newitz predicted an interesting new mix of future jobs for journalists: hacker-journalists (filling roles analogous to those of early war photographers), data-mining reporters (like muckrakers a century earlier), and crowd engineers (including pollsters and census takers). Good information for future journalists seeking jobs. But this assumes that there will be jobs to be had and people willing to take them.

Will there be a future for genuine investigative journalism? Is there a future for investigative journalists?

STAKEHOLDER JOURNALISM AND CULTURES OF FEAR

As I write this column, cyberspace is a-twitter over a misunderstanding between legendary *Washington Post* reporter Bob Woodward and Gene Sperling, the current director of the National Economic Council. When Woodward attributed authorship of the 2012 budget sequestration concept to the White House, Sperling responded via email, saying, "… I think you will regret staking out that claim."

Prior to Watergate, such an exchange would easily have blended into the stew of Washington hubris and hyperbole, but no longer. Now journalists are much more sensitive to subtle signals and threats.

Watergate summary

The Watergate story has been so carefully documented that it has taken on the character of an epic saga. Here's a shorthand account that provides the context for the Sperling-Woodward exchange.

Associate FBI director William Mark Felt ("Deep Throat") aided Bob Woodward and fellow *Washington Post* reporter Carl Bernstein in their investigation that uncovered illegal activities associated with Richard Nixon's presidency, including, but not limited to, burglary, illegal wiretapping, money laundering, obstruction of justice, perjury, and misuse of public funds.

The Nixon administration responded to the charges with denials and warnings, including the threat to prosecute Woodward and Bernstein under the 1917 Espionage Act—the same law that sent the Rosenbergs to the electric

0018-9162/13/$31.00 © 2013 IEEE

chair, put Samuel Loring Morison in prison, and currently is being used to prosecute Bradley Manning. This isn't the kind of law that anyone wants to get on the wrong side of—whether soldier, spy, or journalist.

Fortunately for Woodward and Bernstein, the *Washington Post* was secure enough financially and strong enough politically to deflect attacks from the White House. But just to be on the safe side, editor-in-chief Ben Bradlee had the journalists give their notes to publisher Katharine Graham for safekeeping (his so-called grandmother defense). He believed that Graham was both too influential for the Nixon administration to take on and too sympathetic as a witness for a jury to convict.

Since Watergate, journalism has become more dramaturgic, orchestrated, undifferentiated, and uninspired.

This incident illustrates just how high the stakes were in reporting government misconduct even in the days of relatively unobstructed journalism. It's also worth noting that Nixon was but one security guard and a few tape recordings ("the smoking gun") away from repudiable denial and avoidance of three articles of impeachment.

A changing profession

Since Watergate, journalism has become more dramaturgic, orchestrated, undifferentiated, and uninspired. Independent newspaper publishers and media outlets are harder to find these days. And as time has shown, investigative journalism isn't the ideal instrument of global corporate interests—it's losing out to agenda-based, stakeholder-friendly reporting.

As Newitz observed, journalism is becoming net-centric. This is both blessing and curse—a blessing in terms of ease-of-access of information, a curse because journalists haven't mastered the tools of the networked world, especially the tools that might protect them.

While there are some state protections for journalists, the law of the land is still Branzburg v. Hayes, in which the US Supreme Court held that there's no First Amendment privilege that automatically accrues to reporters—either testimonial or to protect their sources.

The fact that federal courts have considerable latitude in interpreting the Branzburg ruling has, in and of itself, had a chilling effect on journalists who report on controversial topics or challenge established authority. Consider, for example, the case of Valerie Plame, in which at least four members of the George W. Bush administration outed her as an undercover CIA agent—a clear-cut violation of the Intelligence Identities Protection Act, Title VI of the National Security Act of 1947. The only person to serve jail time as a result of "Plamegate" was a *New York Times* reporter who covered the story—for failing to disclose her sources.

Recently, blogger Josh Wolf was imprisoned for seven months for failing to turn over his home movies of a protest at a G8 summit. *San Francisco Chronicle* reporters Lance Williams and Mark Fainaru-Wada were sentenced to 18 months in federal prison for refusing to name sources on the BALCO scandal involving the use of banned, performance-enhancing substances by Major League Baseball players.

The fact that the government is willing to incarcerate reporters over scandals in our national pastime shows the extent of the problem that journalists face. The office of Bush Attorney General Alberto Gonzales argued that the Espionage Act can be used to prosecute individuals who distribute information "not to foreign governments or spies but to 'persons not entitled to receive it'"—that is, investigative reporters.

Extrajudicial threats

As chilling as Branzburg is, it pales in comparison to extrajudicial threats to journalists. In some areas of the world, journalists are murdered with impunity. According to the Committee to Protect Journalists 2012 risk list, this isn't limited to failed states and regions in conflict, but includes countries that claim to be democratic by Western standards, including Brazil, Ecuador, and Turkey (www.cpj.org/2013/02/attacks-on-the-press-cpj-risk-list.php).

Approximately 100 journalists are murdered each year. And even if journalists are spared death, their lives and careers can be ruined if the subject of their reporting is a government or powerful business interest. Examples include Gary Webb, who reported on the CIA involvement in Iran and the LA crack epidemic; Donald Woods, who reported on the murder, and subsequent cover-up, of Steven Biko in South Africa; and Nick Davies, who was brought before a parliamentary review panel for breaking the *News of the World* phone-hacking scandal.

While wealth and celebrity can insulate contrarians from persecution, journalistic license doesn't count for much these days. Don Henley can take on Rupert Murdoch in song without effect, but not a reporter for *The Guardian*. Even Helen Thomas, Phil Donahue, and Dan Rather lost their positions over personal expression.

POST-WATERGATE JOURNALISM AND TECHNOLOGY

The current mantra of media critics and commentators is that the new standard-bearers of post-Watergate journalism are online. There's no denying that citizen journalism, blogs, news portals, subscription-push services, and the like can be valuable immediate news sources. But they also can be sources of misinformation, propaganda, bias, and hatemongering (http://martinlutherking.org).

The media critic's mantra ignores the enormous value that a large newsroom of dedicated professional journalists adds to a story. Without them as a filter, every online reader would need to hold a black belt in what Howard Rheingold calls the "art of crap detection." The public isn't capable of rising to this challenge.

The suggestion that online fact checkers can take up the verification slack is misguided: the public isn't willing to invest the time to use them properly; there's no easy way to vet them; and in principle, they're no more reliable than the original sources.

The Internet is truth- and value-neutral. It's no more a conduit for honesty and justice than the loudspeaker. The Internet's benefit is that it offers convenient, rapid access to data. Determining whether the data is reliable or valuable, true or false, is a nontechnological issue that requires independent consideration.

TEN GRAND CHALLENGES FOR FUTURE JOURNALISTS

Too much attention is being paid to the survival of the business of journalism, and not enough to the survival of journalists. The real problem we should be addressing isn't whether click-and-banner or pay-wall business models are optimal, but whether the next generation of journalists will be able to effectively practice their profession. Ironically, the very technology that the media pundits suggest might get journalism out of the hole actually might be making the hole deeper.

URL PEARLS

Annalee Newitz is a freelance writer and lead editor on io9.com, a science fiction and science blog. From 1999 to 2008, she wrote the syndicated column, Techsploitation (techsploitation.com). Lindsay Oberst offers a similar perspective at http://sustainablejournalism.org/future-of-journalism/journalism-jobs-may- hold-future.

Hal Varian provides some useful information on the economics of journalism at http://cdn.theatlantic.com/static/coma/images/issues/201006/hal_varian_presentation.pdf.

For an extensive analysis of Branzburg v. Hayes and reporter shield laws (or absence thereof), see Leslie Siegel's "Trampling on the Fourth Estate: The Need for a Federal Reporter Shield Law Providing Absolute Protection against Compelled Disclosure of News Sources and Information": http://moritzlaw.osu.edu/students/groups/oslj/files/2012/04/67.2.siegel.pdf.

For more information on threats against journalists, see

- **the Knight Center for Journalism in the Americas: http://knightcenter.utexas.edu/category/topics-blog-en/threats-against-journalists),**
- **the Committee to Protect Journalists:www.cpj.org,**
- **and Reporters without Borders: http://en.rsf.org.**

The London School of Economics has an interesting site on media policy: http://blogs.lse.ac.uk/mediapolicyproject/programme.

For more on former Attorney General Alberto Gonzales's interpretation of the Espionage Act, see Derigan Silver's article at www.tandfonline.com/doi/abs/10.1080/10811680802388881.

Fact checking:

- **Online fact checkers fall under the category of trusted source networks. "Trust" should be used with care in this context. Some of the more popular sites include: the Annenberg Public Policy Center's FactCheck.org site (www.factcheck.org) and The Washington Post (www.washingtonpost.com/blogs/fact-checker). Post columnist Glenn Kessler also has a Fact Checker column.**
- **At this writing, The Washington Post has a prototype multimedia version online at http://truthteller.washingtonpost.com. This prototype isn't quite ready for prime time, but the concept is superb.**
- **A metalevel fact-checking source is available from the Poynter Institute: www.regrettheerror.com.**
- **A more democratic "smart mob" fact checking approach might be a useful addition. The challenge here would be to develop the aggregating and filtering technology. Howard Rheingold describes such things in Crap Detection 101: How to Distinguish Good and Bad Information Online (O'Reilly Media, 2011). Rheingold also offers a mini course in crap detection that's well worth the time to watch: http://rheingold.com/2013/crap-detection-mini-course. In Rheingold's view, crap detection is a core literacy skill along with attention, participation, cooperation, and network awareness.**

Future journalists should avoid the following circumstances:

- prosecution under Branzburg v. Hayes, the Espionage Act, and the Patriot Act;
- receiving national security letters;
- receiving administrative subpoenas;
- being placed on TSA no-fly and selectee lists;
- having a passport revoked;
- 24/7 surveillance;
- barratry and strategic lawsuits against public participation (SLAPP suits);
- incarceration; and
- exile.

Too much attention is being paid to the survival of the business of journalism, and not enough to the survival of journalists.

In addition, they should plan to become self-sustaining for long enough to have time to develop a story.

The first seven are potential threat vectors for future journalists that indirectly involve modern technology. Absent a sudden and unexpected reversal in the direction that the US Congress and Supreme Court are headed, technology must play a part in sustaining the status and well-being of investigative journalism.

It would be foolish to believe that repeated Freedom of Information Act requests about sensitive topics—in terms of both national security and politics—would go unnoticed and unrecorded. It should also be remembered that the National Security Agency's warrantless wiretapping didn't end when the Bush administration bowed to public pressure and ceased the program in 2007. Congress simply amended the Foreign Intelligence Surveillance Act in 2008 to accommodate wiretapping without a presidential executive order—albeit with some minimal restrictions like requiring the agency to request FISA court approval within seven days or the evidence might be inadmissible.

The FBI has reportedly asked Congress to extend the Communications Assistance for Law Enforcement Act to require ISPs and social network, Web email, and VoIP providers to give the FBI a "surveillance backdoor" (http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now), with the intent of having every application and service shipped "wiretap ready." Is this the kind of environment that will nurture and sustain investigative reporting?

GRAND SKILLSETS FOR FUTURE JOURNALISTS

To counter these sorts of threats, future journalists must be much more sophisticated in their use of technology—but not in the sense that Annalee Newitz meant. To meet the grand challenges, they might need some grand skillsets, including the following:

- use anonymizers,
- use remailers,
- make a commitment to whole-message-encryption of email,
- make a commitment to end point file encryption,
- develop the ability to get credit or compensation for non-attributable bylines, and
- cultivate a background in criminal law and develop a close working relationship with successful First Amendment attorneys.

The first four skills raise the bar on privacy protection—not just for journalists, but for everyone.

At this writing, the Tor implementation of onion routing is the anonymizing service of choice (www.torproject.org/about/overview). Although frequently thwarted by foreign governments like those in China and Iran, as well as an occasional western intelligence service, it's still the benchmark for secure use of the Internet.

Remailers work in a fashion similar to anonymizers. In both cases, the technology defines a communications architecture that conceals relationships between participants and contents. Anonymizing services are viable if, at a minimum, they employ forward secrecy, reply blocks, chaining, and strong encryption and don't use logs or identity lists. End point file encryption should be in use in all computer systems.

Future journalists must understand how various privacy-preserving environments work because they all aren't optimal at any given moment, and all are vulnerable to attack. There are many slips twixt cup and lip in the privacy biz.

In the future, telling a story might become less important than maintaining personal anonymity after it's told. Bylines currently make reporters big targets for those who would do them harm: drug cartels, revolutionaries, criminals, authoritarian/dictatorial governments, and the like. This can only get worse in time unless the world takes an about-turn toward "playing nice." Journalists would be well advised to build some measure of anonymity into their compensation and rewards structure—just in case. And it never hurts to "lawyer up."

Neil Postman compared George Orwell and Aldous Huxley this way: "What Orwell feared were those who would ban books. What Huxley feared was that there would be no reason to ban a book, for there would be no one who wanted to read one." The modern paradigm of this Orwell-Huxley dystopia isn't limited to places like North Korea and Eritrea, where there's nothing even remotely approaching objective journalism.

The importance of the fourth estate of which Edmund Burke and Thomas Carlyle were so enamored is neither universally recognized nor valued. And this lack of appreciation isn't limited to failed states or dictatorial regimes. It has little appeal to those who favor intrusive governments that view a free press as outside constitutionally mandated systems of checks and balances. For them, the prosecution of journalists who might seek to expose political wrongdoing is consistent with their view of democracy.

The paradigm that Postman described must be amended to include a technological framework for journalists. If objective journalism is to survive, we might need to shift the discussion away from media companies that cater to their marketing departments and are preoccupied with profits and revenues to a discussion of how we need to protect the journalists who make the enterprise viable.

The defensive measures presented here are a start. If computing technology is to help save the day, journalists must ratchet up their skill levels, and computing professionals must become more sensitive to their future needs.

This is also a good time for journalists to begin supporting the technology that will help sustain their industry. Focused, genuinely interdisciplinary journalism informatics programs are a start, along with J-school affinity groups like Journalists for Tor or Anonymizers R Us. But an appreciation of the problem will generate much of the needed momentum.

Hal Berghel, *Out of Band column editor, is a professor of computer science at the University of Nevada, Las Vegas, where he is the director of the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). Contact him at hlb@computer.org.*