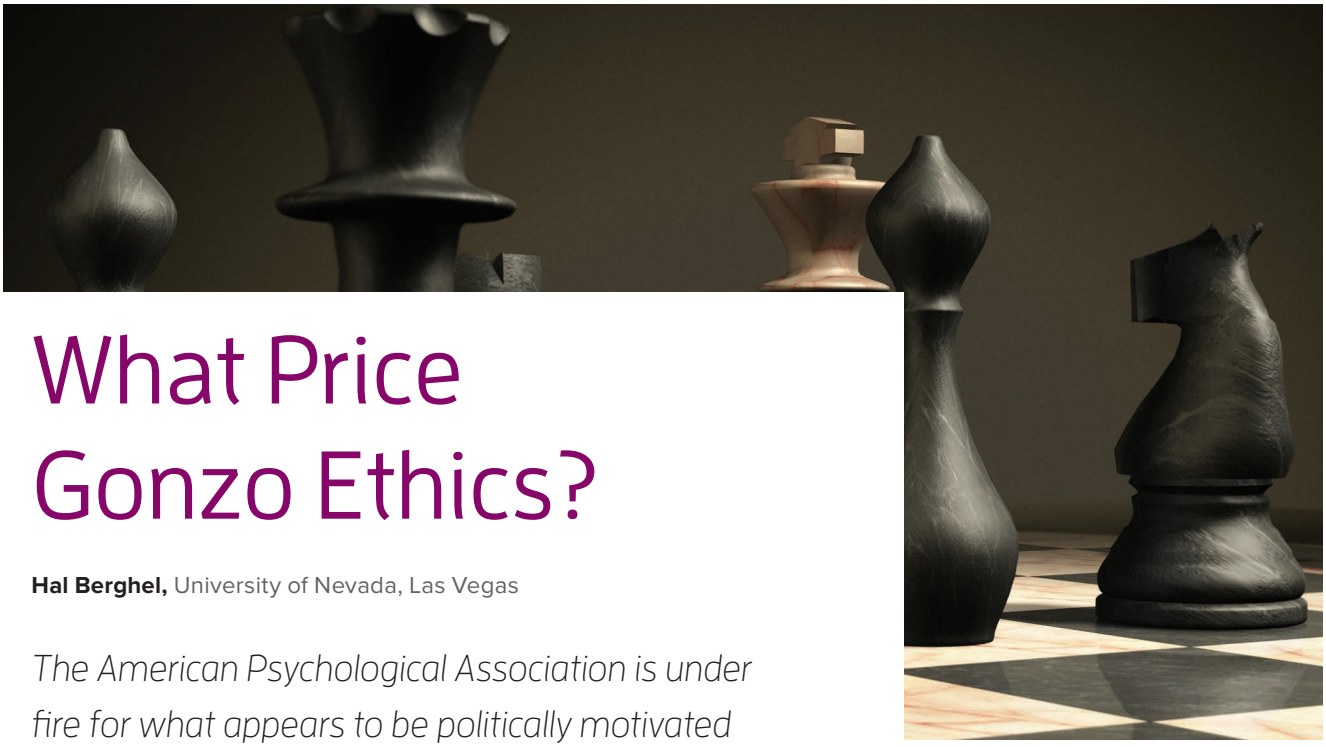

What Price Gonzo Ethics?

Hal Berghel, University of Nevada, Las Vegas

The American Psychological Association is under fire for what appears to be politically motivated ethics-skewing gone wild. To avoid the same shameful fate, professional societies are well advised to reexamine their own code of ethics.

On 20 April 2015 *New York Times* journalist James Risen published a revealing article on the relationship between the American Psychological Association (APA) and those involved in the torture of post-9/11 prisoners. This created a tsunami of bad publicity for the APA. This story relates to all professionals, not just psychologists.

DO NO HARM?

The principle of nonmaleficence has been a cornerstone of patient-care ethics since Hippocrates. In this case, it is Principle A of the *Ethical Principles of Psychologists and Code of Conduct*'s General Principles.[1] The Hoffman Report (as it's commonly known),[2] recently commissioned by the APA, shows that this principle was subverted under the Bush/Cheney administration's torture program; complicit in this were the psychologists who sought government support and largesse therefrom. The Hoffman Report demonstrates how corrosive the Bush/Cheney administration's policies were on the nation's moral fabric. It's reminiscent of US supersecret mind control/chemical weapons projects ARTICHOKE, MKDELTA, MKUltra, 112, as well as the KUBARK interrogation techniques; if you throw in COINTELPRO tactics and a bit of Spanish Inquisition, you get the flavor of things. (For a more complete history of the US Central Intelligence Agency's [CIA's] dark programs, see David Talbot's recent book, *The Devil's Chessboard*.[3])

The first attempt to establish rules governing the treatment of detainees following the 9/11 terrorist attacks was set forth by two lawyers in John Ashcroft's Department of Justice on 30 November 2001 (www.aclu.org/sites/default/files/field_document/20011131_yoo_delahunty_memo.pdf). In this memorandum, attorneys John Yoo and Robert Delahunty articulated the position that the UN International Court of Justice's interpretation of the Geneva Convention is too expansive, and that the Bush/Cheney administration's mere accusation that an individual is a terrorist would automatically preclude qualification for "elementary considerations of humanity" referenced under Common Article 3 of the Geneva Conventions. Yoo and Delahunty argued that neither the framers of Article 3, nor those of the US Constitution, anticipated post-9/11

0018-9162/15/$31.00 © 2015 IEEE

EDITOR **HAL BERGHEL**
University of Nevada, Las Vegas; hlb@computer.org

circumstances, hence these restraints couldn't possibly apply to al-Qaeda and Taliban detainees. This memo also set forth a president's limitless authority as Commander in Chief with respect to military commissions. Armed with this power, the Bush/Cheney administration issued many "torture memos" that gave legal cover to those involved in these practices.

The CIA and the Department of Defense (DoD) were already using "counter-resistance strategies" (a euphemism for torture; see http://whenhealersharm.org/wp-content/uploads/20021002-counter-resistance-strategy-meeting-minutes.pdf), which were reverse-engineered from the Navy's Survival, Evasion, Resistance and Escape (SERE) training manual,[4] which is indebted to Nazi Gestapo techniques dating back to the 1930s and 1940s. As a matter of fact, the term "enhanced interrogation" was actually borrowed without attribution from the German *verschärfte vernehmung*. However, note that the Gestapo initially prohibited the hypothermia and waterboarding torture methods that became so popular at Gitmo and CIA black sites. In addition, the Gestapo was also more explicit regarding potential victims: "... the sharpened interrogation may be applied only against Communists, Marxists, members of the Bible-researcher sect, saboteurs, terrorists, members of the resistance movement, parachute agents, asocial persons, Polish or Soviet persons who refuse to work, or idlers" (www.theatlantic.com/daily-dish/archive/2007/05/-versch-auml-rfte-vernehmung/228158).

PROFESSIONAL HELP

All went well until 2004, when leaks about the torture program led to public outcry. Administration officials found secret-memo legal cover wanting, so they couched their responses in humanistic terms to reassure the world and the alarmed public that these weren't war crimes. In Bush's words: "The United States does not torture. It's against our laws and it's against our values. I have not authorized it and I will not authorize it" (www.washingtonpost.com/wp-dyn/content/article/2006/09/06/AR2006090601425.html). The solution was to attract compliant (read: unquestioning) oversight from credible sources outside the administration and to leverage that faux blessing into a cover story. It went something like this: the APA says that what we do isn't torture, and we stand by their opinion.

In 2005 the APA president formed a national security and psychological ethics task force heavily populated with those either in or connected with military and intelligence communities to craft a position on this issue that could be of help to the administration. The result was the now-famous Psychological Ethics and National Security (PENS) report[5] that reversed the APA's prior stance against torture and other cruel, inhuman, degrading treatment or punishment. PENS set new standards: it was now acceptable to participate in activities that violated the APA's code of ethics when such activities were consistent with the law of the governing legal authority. The torture memos set up the required legal framework and requisite cover for the perpetrators. To ensure that this change in stance didn't gain legs prematurely, disclosure to the APA membership and any note taking on the part of task force participants was strictly forbidden (www.salon.com/2006/07/26/interrogation_3).

However, one invited participant, Jean Maria Arrigo, was so aghast at the administration's creative new uses for psychologists in the torture program that she sent the report, related email communications, and personal notes to both the Senate Armed Services Committee (www.democracynow.org/2007/6/1/the_task_force_report_should_be) and journalist Katherine Eban (www.vanityfair.com/news/2007/07/torture200707).

Independently, an internal military report by US Navy general counsel (GC) Alberto Mora—protesting the new torture policy to Defense Department general counsel William Haynes II—was reported by journalist Jane Mayer for *The New Yorker* (www.newyorker.com/magazine/2006/02/27/the-memo) and Mark Benjamin for *Salon.com* (www.salon.com/2006/07/26/interrogation_3). This set the stage for an existential crisis within the APA. The APA's initial response was to engage in "deception four-step"—ignore, deny, ridicule, condemn—and Jean Maria Arrigo was its first victim (www.theguardian.com/law/2015/jul/13/psychologist-torture-doctors-collusion-jean-maria-arrigo). Of course, even if the Bush/Cheney torture program hadn't been legitimized, had a participant been arrested by the International Criminal Court for war crimes, the US could always have fallen back on the Hague Invasion Act and attacked the Netherlands (hrw.org/news/2002/08/03/us-hague

> The APA scandal shows how easy it is to subvert a professional code of ethics under pressure from powerful external influences.

-invasion-act-becomes-law). It's always good to have a backup plan.

Fortunately, several years of Risen's investigations finally culminated in his 2014 book *Pay Any Price: Greed, Power, and Endless War*,[4] bringing additional visibility to the issue. The APA responded with denials (www.apa.org/news/press/response/risen-book.aspx); however, upon release of the Hoffman Report, the tables were turned (www.apa.org/independent-review), the APA leadership was pressured into action, and ultimately this led to an unprecedented resignation of several APA executives in 2015. The APA's executive council passed a resolution barring members from participating in military interrogation. Oh, what a tangled web the APA wove (http://ethicalpsychology.org/materials/Behnke-Fact-Sheet-Feb2011.pdf; www.theguardian.com/world/2014/jan/22/guantanamo-torture-mohammed-al-qahtani-suspected-9-11-hijacker)! I would be remiss if I didn't acknowledge that the most sustained coverage of this entire affair was provided by DemocracyNow.

BLOWING WHISTLES OR BLOWING CAREERS

The APA scandal is a noteworthy example of how a code of ethics can be easily subverted when the parent organization submits to the will of the authoritarian elite. In this case, it eventually backfired as the Hoffman Report was sufficiently embarrassing to incentivize the APA to clean house. But it shouldn't have gone that far. Many psychologists knew what was going on, but for various reasons refused to speak out; others spoke out but were silenced. The Hoffman Report shows what happens when iconoclasts are intimidated into silence. Perhaps it's time for all professionals to investigate whether their respective societies have been so compromised.

Lest we be tempted to cast stones at our APA sisters and brothers, perhaps we should look at our own codes of ethics and see how well we're doing. There are several that we can pick from: IEEE (www.ieee.org/about/corporate/governance/p7-8.html), ACM's software engineering code (www.acm.org/about/se-code), and ACM itself (www.acm.org/about/code-of-ethics). I'll focus on the ACM code, because that's the one I'm most familiar with.

> The intelligence agencies' conduct seems at odds with the spirit of the ACM code.

ACM's code of ethics consists of 24 imperatives organized in 4 sections. For our purposes, discussion is limited to section 1: General Moral Imperatives, beginning with subsection 1.2 (www.acm.org/about/code-of-ethics/#sect1), which is about avoiding harming others:

> *"Harm" means injury or negative consequences, such as undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm to any of the following: users, the general public, employees, employers. It's often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others. If system features are misrepresented to users, coworkers, or supervisors, the individual computing professional is responsible for any resulting injury. ... [T]he computing professional has the additional obligation to report any signs of system dangers that might result in serious personal or social damage. If one's superiors do not act to curtail or mitigate such dangers, it may be necessary to "blow the whistle" to help correct the problem or reduce the risk.*

Although this section rings true to me, abiding by it in the current surveillance state could get a computer professional prosecuted under the Espionage Act. The familiar three-letter-acronym intelligence agencies obviously won't warm up to subsection 1.2 of the ACM code of ethics any time soon. It's well documented by Edward Snowden and others that the US National Security Agency (NSA) systems were frequently misrepresented to both users and coworkers, not to mention Congress. But, and here's the rub, this misrepresentation wasn't just for national security purposes, but also to conceal illegality—specifically, violations of the Bill of Rights.

Note that under subsection 1.2 the computing professional has the additional obligation to report anything that might result in serious personal or social damage, even if it requires blowing the whistle. That is in fact what William Binney (NSA communications intelligence director), Thomas Drake (NSA executive), and J. Kirk Wiebe (NSA senior analyst) did—after first alerting their superiors—but that was fruitless, and they were later raided by NSA agents; and Drake was even prosecuted under the Espionage Act (www.usatoday.com/story/news/politics/2013/06/16/snowden-whistleblower-nsa-officials-roundtable/2428809). In addition to the scores of scholarly books on this subject, this turn of events at the NSA was also the focus of an episode of *Frontline* in 2013 ("The United States of Secrets," WGBH, PBS; www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-j-kirk-wiebe), and online magazine *Tragedy & Hope* also posted an excellent interview with William Binney (www.youtube.com/watch?v=3owk7vEEOvs).

I call your attention to the parallel here with the torture program: NSA

whistleblowers did what Mora did with regard to the torture program. Like Mora, NSA staffers Binney, Drake, and Wiebe worked within the system and reported wrongdoing to their superiors. And like Mora, they were informed that the Bush/Cheney administration had approved the programs these staffers believed were unconstitutional, thus their opinions were no longer relevant and their future careers would depend on their silence.

So how does this scenario fit within section 1.2? The intelligence agencies' conduct seems at odds with the spirit of the ACM code. So for computing professionals employed by them, should the code be modified to comply with government expectations? This is where things get dicey. To reconcile ACM's code with the conduct of these agencies, it would appear that we would have to add wording to the effect that code violations are acceptable whenever "such activities were consistent with the law of the governing legal authority," as the APA did. We would be remiss if we failed to appreciate the lack of success that the APA had with this tactic.

MARKETPLACES OF DECEPTION

Subsection 1.3 holds that "the honest computing professional will not make deliberately false or deceptive claims about a system or system design." How does that language fare against the NSA's aggressive use of zero-day exploits against nonmilitary targets (see my column "A Farewell to Air Gaps, Part 2," *Computer*, July 2015, pp. 59–63)? Virtually every representation that the NSA leadership made about the bulk metadata collection program indicates that it violates this principle. If we're to use a national security exemption here, we should be mindful of potential moral hazards resulting therefrom lest we exempt all responsible resistance to corrupted systems under this ill-defined and undocumented banner. Let's be very clear about this: recent experience has shown that administrations claim national security privilege for virtually everything done in their name that might prove embarrassing or expose illegality. If codes of ethics are to comply with any and all claims of national security protection, under the current climate that amounts to near-total censorship reminiscent of past totalitarian regimes. So some refinement is called for, especially in cases when employer directives are inconsistent with constitutional guarantees. And if exemptions are tolerated, just how far down in the org chart does this exemption flow, and in what directions?

Moral responsibility and autonomy in decision making tend to be undercut by nondisclosure agreements (NDAs), security clearances, and draconian employment contracts—all of which are nearly ubiquitous in today's technology sector. Matters are much worse for employees-of-conscience in the US due to the additional encumbrance of the common law employment-at-will doctrines. We should also note that covenants of good faith and fair dealing have little to no effect on security, investigative, and intelligence communities in which employee access to courts, records, and, ultimately, justice, is curtailed.

The authors of the ACM code of ethics probably did not anticipate a world in which sovereign states could be in a permanent state of digital aggression against their own citizens. Where is the balance between our responsibilities under NDAs, oaths, clearances, and the like on one hand, and our moral responsibilities on the other? This isn't unlike APA's swerve off the ethical track: the PENS report specifically stated that government authority trumped ethical considerations when it comes to torture programs.

Should computing professionals be prepared to accept NDAs and loyalty oaths when in conflict with the Constitution? Or should our commitment be more categorical? I don't know, but I think we should have a discussion about it.

Finally, we deal with the subject of subsection 1.7: respecting others' privacy. I think you see where this is headed: "It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals .... Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies." This naturally begs the question of how this fits with the Federal Bureau of Investigation's (FBI's) Carnivore (www.vjolt.net/vol6/issue2/v6i2-a10-Jennings.html) and Magic Lantern (www.kaspersky.com/news?id=266) programs, and the NSA's bulk metadata collection program.

WHERE DO WE GO FROM HERE?

In light of the recent APA controversy, I'm convinced that this is a good time for professionals to revisit their codes of ethics. A brief review of computing's recent history shows this.

With the advent of the Internet, data self-determination came under threat as a variety of interests sought to capitalize on exceedingly convenient access to information. For the past few decades, data protection has typically been associated with object-level data. But the Snowden revelations confirm that threats in fact now include metadata issues; location independence; sensor networks resistance; and a cornucopia of malware that compromise data integrity, personally identifiable

> Arguments that the Constitution is trumped by an agreement you make with your employer are indefensible.

ETHICS RESOURCES IN COMPUTING

Significant concern about computing-related ethics began in the middle of the past century. In 1966, the International Federation for Information Processing (IFIP) supported a comparative analysis of 30 codes of ethics and conduct relevant to the information technology professions (www.ifip.org/36years/a53berlr.html). In 1992, Ronald Anderson conducted a similar study of the ethics of computing professionals, focusing in particular on ACM's code of ethics (*Social Science Computer Rev.*, vol. 10, no. 4, 1992, pp. 453–469).

IEEE's symposium entitled Ethics in Engineering, Science and Technology (http://sites.ieee.org/ethics-conference) includes tracks on ethics in whistleblowing, regulation, and computing societies. IFIP has also featured ethics in its Human Choice and Computers (HCC) conferences since 1974 (http://hcc12.net). ACM's Special Interest Group on Computers and Societies is also focused on this area and has existed for many years (www.sigcas.org).

information, individual privacy, and so forth.

Given the complexity of today's highly networked computing infrastructure, ethical use for the betterment of society must—out of necessity—be a shared responsibility among those who commission the activity, those who produce the computational artifacts, and those who deploy it. At each stage, the questions of legality and morality, especially in terms of potential negative externalities, must be addressed.[6] Both "dissipation of responsibility" and "diffusion of responsibility" are relevant to this issue.[7]

Any computing-related code of ethics must include a discussion of open government in this context; and no government can be "free and open," nor will its decision making be transparent, when virtually everything is classified, behind a draconian firewall, and protected by security clearances blocking any semblance of legitimate oversight. It would appear that we're at a decision point: either change our code or change our government's policies. For some additional resources on this issue, see the "Ethics Resources in Computing" sidebar.

LOYALTY LIES

I'll conclude with an example of how convoluted moral positions can become when forced through ideological funnels. Joel Brenner was the NSA's inspector general and head of counterintelligence in the Bush/Cheney administration. In a recent article,[8] Joel Brenner argues employee oaths to government agencies like the NSA, CIA, and FBI should trump any oath to Congress. He used the example of the time when former CIA director Richard Helms lied to Congress about CIA involvement in the 1973 overthrow of the Chilean government under legitimately elected president Salvador Allende. Brenner likened Helms's case to that of intelligence official James Clapper, who in 2014 lied to Congress about whether the NSA collects "any type of data at all on millions or hundreds of millions of Americans." Clapper, unlike Helms, was not testifying under oath, so perhaps no legal issue was violated in his case. However, his deceit might have been prosecutable under the laws of false statements, false declarations, obstruction of justice, and so on, even if perjury wasn't involved. Brenner's claim, however, is that both Helms and Clapper were "honor bound" to lie to Congress because their oath to their agency is of a higher order. This line of argument, no matter how offensive it might be, must be taken seriously because it's so widespread among the controlling elite. Of course there's only one oath recognized in the US Constitution, and that is to preserve, protect, and defend the Constitution. Any argument that the Constitution is trumped by an agreement you make with your employer is ungrounded in the law, self-serving, and indefensible.

Furthermore, the Constitution makes an allowance for such matters in the Fifth Amendment. Both Helms and Clapper could have responded in any of the following ways:

- I cannot answer that question without possible self-incrimination.
- I cannot answer that question without subjecting myself to prosecution.
- My agency oath prevents me from answering that question.
- My agency requires that I answer such questions in a secret session in accordance with Article 1, Section 5, of the Constitution.

Any of these responses would have prevented them from lying to Congress. Brenner claims that for Helms and Clapper to have invoked these protections would have strained their own credibility. However, *lying* is a real credibility strainer—gonzo moralists need to learn to live with this as they practice their brand of gonzo testimony.

This point illustrates that there's plenty of opportunity for conflict to arise among codes of ethics, oaths, rules, NDAs, security clearances, and so on. If a code's whistleblower clause is to have any meaning at all, it must work within the constraints imposed by

employment oaths, NDAs, and the like. If we deny this fundamental equipotence, we might as well strike the clause and include "lying under oath" in job requirements.

REFERENCES

1. "Ethical Principles of Psychologists and Code of Conduct," American Psychological Assoc., effective 1 June 2010; www.apa.org/ethics/code/principles.pdf.
2. D. Hoffman et al., *Independent Review Relating to APA Ethics Guidelines, National Security Interrogations, and Torture*, report to the special committee of the board of directors, American Psychological Assoc., 2 July 2015; www.apa.org/independent-review/APA-FINAL-Report-7.2.15.pdf.
3. D. Talbot, *The Devil's Chessboard: Allen Dulles, the CIA, and the Rise of America's Secret Government*, Harper, 2015.
4. J. Risen, *Pay Any Price: Greed, Power and Endless War*, Houghton Mifflin Harcourt, 2014.
5. "Report of the Presidential Task Force on Psychological Ethics and National Security," report, American Psychological Assoc., June 2005; www.apa.org/pubs/info/reports/pens.pdf.
6. H. Berghel, "Technology Abuse and the Velocity of Innovation," *Cutter IT J.*, vol. 28, no. 7, 2015, pp. 12–17.
7. L.M. Hilty, "Ethical Issues in Ubiquitous Computing—Three Technology Assessment Studies Revisited," K. Kinder-Kurlanda and C. Nihan, eds., *Ubiquitous Computing in the Workplace*, Springer, 2015, pp. 45–60.
8. J. Brenner, *Clapper and Wyden: Scenes from a Sandbagging*, *New Republic*, 2 July 2013; www.newrepublic.com/article/113714/ron-wyden-sandbagged-james-clapper-history-intelligence-oversight.

HAL BERGHEL is an ACM and IEEE Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.