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

Huawei, BIS, and the IEEE: It's Déjà Vu All Over Again

Hal Berghel, University of Nevada, Las Vegas

Once again, the proponents of big and powerful government called on professional societies to do their bidding for them. And, once again, IEEE members nudged the IEEE over to the right side of history.

Government three-letter agencies have a checkered public policy history when it comes to academic freedom and free speech.[1–3] Historically, this position has been bipartisan. The most recent interference that involved the IEEE came from the Trump administration as part of its broader tariff/import-control strategy. Let me emphasize that I take no position on the U.S. government's tariff/import controls or the overall public policy agendas of government agencies; I restrict my comments to the involvement of professional societies, such as the IEEE, in such agendas.

The current example involved a U.S. government action taken against Huawei and 68 affiliates by the Bureau of Industry and Security (BIS) Division of the U.S. Department of Commerce that purportedly "advances… national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system, and by promoting continued U.S. leadership in strategic technologies … by maintaining and strengthening adaptable, efficient, effective export controls.…"[30]

This past May, BIS placed Huawei on its "entity list" for engaging "in activities that are contrary to U.S. national security or foreign policy interests including alleged violations of the International Emergency Economic Powers Act (IEEPA), conspiracy to violate IEEPA by providing prohibited financial services to Iran, and obstruction of justice in connection with the investigation of those alleged violations of U.S. sanctions, among other illicit activities."[31] It isn't altogether clear whether, or to what extent, BIS's claims were legitimate. On 29 June 2019, President Trump reversed some of the BIS decision and announced that U.S. companies can sell equipment to Huawei after all,[4] thereby placing the justification for the May action in some doubt.

To avoid potential digital tribal conflict from partisans, I again emphasize that, for the purposes of this column, I am agnostic regarding the issues of whether BIS is needed, purposeful, effective, or well managed in pursuit of its mission and whether placing Huawei on the entity list was justified.

Digital Object Identifier 10.1109/MC.2019.2927074
Date of publication: 24 September 2019

I restrict my attention to a narrow issue involving one of our professional societies and the Commerce Department's actions as they impact the broader professional computing community.

THE IEEE MEMO

In response to the Commerce Department/BIS announcement, the IEEE issued a "Statement on Participation of Members/Volunteers on BIS Entity List" on 22 May 2019 to "…provide guidance to IEEE volunteers, members, and staff on interacting with a Listed Person or an employee of a Listed Person (or other person directly paid or otherwise sponsored by a Listed Person) who seeks to participate in IEEE activities." As expected, the IEEE reaffirmed some of its core principles as it relates to the BIS announcement, namely that "listed persons"

- "may continue to be IEEE members in good standing and continue to be eligible for membership-grade elevation"
- "may continue to order and receive subscriptions and make other purchases of IEEE publications, as well as access materials publicly available on IEEE *Xplore*"
- "may attend IEEE-sponsored conferences (whether inside or outside of the United States) that are open to interested members of the public. A listed person may speak or make presentations at such conferences and may submit materials for inclusion in such conference proceedings or for publication in post-conference written proceedings (to the extent otherwise permitted under the conference rules)"
- "may participate in business, logistics, and other meetings relating to conference planning or evaluation"
- "may participate in meetings of a leadership group such as executive committees, administrative committees, or similar bodies (or subcommittees of such bodies) for purposes of discussing or voting on business, logistics, nominations, elections, or other aspects of organizational governance"
- "may continue to submit articles and other materials for consideration for publication. IEEE staff and volunteers may continue to provide normal copyediting support"
- "may continue to join or use an email reflector for nontechnical discussions or (where the reflector can be accessed through a publicly available archive) for technical discussions"
- "may provide funds for conference sponsorships, scholarships, or awards."

I would fully expect any professional association to reaffirm such principles in this context, and I take no exception to the IEEE's position. However, the 22 May memo also contained the following IEEE statements that I did take issue with:

- "A listed person shall *not* participate in nonpublic meetings or communications that involve technical discussions."
- "A listed person may *not* receive or access materials submitted by other persons for publication until after IEEE has accepted the material for publication in accordance with IEEE's normal publication process. Once material has been accepted for publication, a listed person may act as editor or peer reviewer for that material."

Ignoring the baroque logic in the strange last sentence, it seems clear that the intent was to minimize any skullduggery that might result from listed persons being involved in editorial decision making. In this second set of points, the IEEE became, perhaps unwittingly and under duress, drawn into a position of agency by the government, a position that it should not relish and, in the future, should avoid. Let me be very clear: it was unwise to put these last two points in print because of the implicature of the statements, not the logical implication. My own position is that it was unwise to send out the 22 May memo at all! This sort of thing happens when you give attorneys keyboards. (I am confident that this memo was not inspired by the IEEE membership!)

In the end, sensible minds prevailed. On 2 June, IEEE President José Moura walked back from the 22 May memo and announced via email to IEEE members that, subsequent to feedback from the membership, the IEEE "has revised our guidance to remove any restriction on the participation of the employees of these companies as editors or peer reviewers in the IEEE publication process. To reemphasize, all IEEE members can continue to participate in the open and public activities of the IEEE, including our scientific and technical publications." This is what most of the IEEE membership would have assumed all along. In the end, the original memo accomplished nothing from a policy point of view.

Once again, the IEEE was brought into alignment with the right side of history—not by lawyers, but by pressure from the membership. Moura confirmed this in his email. However, several aspects of the IEEE reaction to the BIS announcement are alarming and deserve further discussion, not the least of which whether the 22 May memo was necessary and proper for a professional society in the first place. Moura claimed that it was necessary to "protect [IEEE] volunteers and members from potential legal risk that could have involved significant penalties." His email begins to run off the rails with his remark that, "As a nonpolitical, not-for-profit organization registered in New York, IEEE must comply with its legal obligations under the laws of the United States and other jurisdictions." I leave it to legal scholars to determine whether agency is required for such compliance. I know of no case law that holds that professional organizations are responsible for their membership's behavior as a registered not-for-profit organization in this way. This situation is not bound by the Racketeer Influenced and Corrupt Organizations Act (i.e., RICO) statutes. By way of full disclosure, I am not a lawyer. If such case law exists, please send me the links; I'll verify and follow up in an appropriate venue.

DÉJÀ VU

The IEEE and other professional computing societies have dealt with such bureaucratic interference from the U.S. government before. I'll document only one example here, although I have written about others.[5–7]

In the early 1980s, National Security Agency (NSA) Director Bobby Inman tried to coopt Association for Computing Machinery (ACM) and IEEE conferences by laying claim to prepublication censorship for all scholarly papers involving cryptography. A compromise was reached by a committee of representatives from the professional societies that publish cryptographic research (including ACM, the IEEE Computer Society, and the IEEE among others). This compromise encouraged voluntary self-censorship. The only dissenting vote was from IEEE Computer Society representative George Davida,[8] who prophetically predicted that such incursions into the academy could undercut First Amendment protections and, ultimately, subvert scholarship. As I noted in an earlier *Computer* column, history has been very supportive of Prof. Davida's predictions.[5]

Davida emerges as one of the heroes of a story that began a few years earlier, when Inman was appointed to lead the NSA and one of his civilian subordinates, Joseph Meyer, "wrote a threatening letter to the Institute of Electrical and Electronics Engineers, the nation's largest professional engineering society… warning that those planning to participate in an upcoming IEEE symposium on cryptology might violate the law."[3] Apparently, the U.S. Department of State was invoked in this case as the government's interested party. According to Meyer, the State Department's International Traffic in Arms Regulations (ITAR) also extended to all "unclassified data associated with the restricted equipment." By offering conferences on cryptography, he argued, "the IEEE could find itself in technical violation of ITAR." It was clear that Meyer was moving the NSA (and Inman) closer to active censorship of ACM and IEEE conferences.

The IEEE and other professional computing societies have dealt with such bureaucratic interference from the U.S. government before.

According to Bamford,[3] Meyer's letter motivated the IEEE to urge participants in the upcoming conference to clear any questionable material with the U.S. government. This, in turn, produced a storm of controversy both for the IEEE and the NSA, which caused the NSA to disclaim the letter and the IEEE to walk back on its position. The similarities between this incident and the current one should not be overlooked. Again, pressure from the membership worked to the IEEE's advantage.

There is, of course, a much broader historical context behind this that has to do with three-letter agencies' attempted corruption of patent and copyright laws, the invocation of the Invention Secrecy Acts of 1917 and 1951, and the 1917 Espionage Acts that Bamford[3] and others document for any interested reader. I emphasize that Inman, Meyer, and their ideological siblings advanced the notion that 1) government censorship involving technology research was necessary for national security reasons and 2) that professional societies and organizations should be coerced into participating in such censorship. Although I'm not confident that the first point could ever motivate good public policy, I am absolutely convinced that the second will always lead to bad public policy. (Compare Berghel.[9])

The second point is a case of throwing the baby out with the bathwater. Coopting for geopolitical skullduggery those organizations that ensure that the democratic objectives of education and research are met and sustained will ensure the failure of both. According to Bamford,[3] Inman wanted the NSA to "receive the same authority over cryptology that the U.S. Department of Energy enjoys over research in atomic energy. Such authority would grant to the NSA absolute 'born classified' control over all research in any way related to cryptology." According to a 1982 article in *The New York Times*, "Bobby R. Inman predicted a 'tidal wave' of outrage when the public learned of the 'hemorrhage of the country's technology.'"[10]

Inman sought to determine how the NSA might exercise prepublication censorship over nongovernmental technical information particularly relating to cryptography, although how Inman proposed to reconcile his position with the Pentagon Papers Supreme Court decision a decade earlier that banned government prepublication censorship[26] isn't obvious. The study group that Inman convened consisted of scholars who represented the relevant professional societies, including the IEEE, the Computer Society, ACM, the Society for Industrial and Applied Mathematics, the American Mathematical Society, the American Association of University Professors, and other interested parties. Overseen by the NSA general counsel, this study group—with one exception (Davida)—recommended in favor of voluntary censorship. We emphasize that the sole dissenter, George Davida (who represented the Computer Society!), opined that this decision might lead researchers "to lose our constitutional freedoms in bits and pieces.... One gets the impression that the NSA is struggling to stand still, and to keep American research standing still with it, while the rest of the world races ahead. The NSA can best perform its mission in the old-fashioned way: Stay ahead of others."[3] It was Davida, the Computer Society representative in the study group, who opposed any form of government censorship of scientific research! For that reason alone, the Computer Society should consider Davida for a special recognition or name a recognition in his honor.

According to Bamford,[3] the story didn't end there. Inman found that the voluntary censorship approach proved to be ineffective and next proposed to corrupt the National Science Foundation (NSF). The first effort involved an attempt by the NSA to wrest control over cryptography research from the NSF. According to Bamford, Fred Weingarten, NSF special projects coordinator for cryptography work, together with Assistant NSF General Counsel Jesse Lasken, simply refused to recognize the NSA's authority in this area. (Add two more heroes to our story.) This is the same Weingarten who testified against the Digital Millennium Copyright Act anticircumvention provisions in May 2000.[27] Weingarten challenged the technological and economic justifications for the government hardening of copyright controls to serve parochial interests. On both counts, Weingarten and Lasken firmly placed themselves on the right side of history, so let's add two more First Amendment heroes and candidates for special Computer Society recognitions.

We should not dismiss Inman's views lightly, but we should cast at least the second one aside with great gusto. Suppose, for the moment, that we agree with the notion that the government has a national security interest in maintaining a monopoly in cryptography. To assume that censoring U.S. research in cryptography will ensure this monopoly is folly unless and until the United States achieves a monopoly on global intelligence in this area. (We'll return to that issue in a few paragraphs.) Failing that, the censorship will simply drive scholarship into the hands of potential adversaries. It is important to remember that much of the leadership in mathematics and the hard sciences that Germany enjoyed until the 1920s didn't emigrate voluntarily—it was forced out of Germany.

One sure way to purge the United States of whatever lead it may have in cryptography or any other scientific field is to censor it. Even if a government could enlist professional societies as willing accomplices, that won't stop the conversation; it will simply force the speakers to find other venues and diminish the global importance of the professional societies. It is the arrogant illusion of intellectual monopoly that always drives such absurd censorship policies. This tactic should be recognized for what it is: a primitive Orwellian defense mechanism that is guaranteed to prove ineffective in the long term.

THE ASSAULT ON PGP

Not to be thwarted by academic freedom arguments, big government made another assault on computing research a decade later when it attempted to prosecute Pretty Good Privacy (PGP) inventor Phil Zimmermann[11] for alleged violations of the Arms Export Control Act.[12] The government's claim was that the act of releasing shareware necessarily incurs liability for any subsequent online distribution by third parties.[13–15] In this case, the Clinton administration sought to minimize the effect of strong cryptography on the U.S. government's communications-interception agenda—especially as it related to foreign communications. It should be remembered that the anemic 56-b Data Encryption Standard (DES), the favorite target for ridicule by Whitfield Diffie and Martin Hellman,[16–18] was an outgrowth of this agenda, for it was the NSA that convinced IBM to reduce the key size of the Feistel network to 56 b in the first place—a key length that was within the NSA's brute-force capability of decryption at the time. Zimmermann's own account appears on his website.[32] Diffie, Hellman, and Zimmermann offer compelling arguments, in their own ways and at different times, that the NSA and other secretive government agencies should never be allowed control over scientific research in cryptography. Their arguments are pragmatic and reinforced by the recent Shadow Brokers hack that released the NSA exploits WannaCry and Eternal Blue.[19,20] It is singularly unwise to vest such concentrations of power and control in secretive agencies that are, by their very nature, not subject to public accountability. History has shown that, due to the enormous capability of a secretive agency (or government for that matter) to conceal, misrepresent, cover up, and deceive, any disclosure of failed missions, illegal and/or unconstitutional conduct, and the like is unlikely to surface at all. Absent whistleblowers and leakers, the public will never find out. This is Senator Moynihan's central concern in his books on government secrecy.[21,22] Moynihan concludes that government secrecy is far more likely to cover wrongdoing and illegality than to preserve, protect, and defend the Constitution and protect the national security interests of citizens. The overall corrosive effects of secrecy in government has been documented for many years.[23,24]

In the case of government censorship of computing research, we have the worst of all possible worlds: not only does it diminish the overall strength of the nongovernmental and public research agenda, it may ultimately be self-defeating, for the censored information may leak from the censoring agencies just as WannaCry and Eternal Blue leaked from the NSA's Vulnerabilities Equities Process (VEP). The Shadow Brokers experience should provide a wake-up call on just how dangerous it is to allow secretive agencies to maintain a VEP vulnerabilities monopoly—this monopoly provides a uniquely tempting target that would not exist were it not for the monopoly. Since the documented history of this incident is cloaked in secrecy, there is no way for the public to determine whether or to what degree VEP was (and is) a really bad idea. This was the same agency that pushed for the reduced 56-b anemic DES key size and also allowed Shadow Brokers to harvest and repurpose a treasure trove of zero-day malware.[25] Had it not been for the NSA's failed policies and misplaced priorities, 1970s cryptographic systems would have been more secure, and the current world's supply of virulent malware in the hands of cybermercenaries would have been diminished. Only authoritarians and dictators consider secretive government agencies as trusted systems.

IN SHORT

This problem will never go away as long as authoritarians are drawn to government. As this goes to press, the Trump administration is considering whether to seek legislation to outlaw tech companies from using end-to-end encryption[28,29] that cannot be broken by Big Brother, reminiscent of the DES-56 discussions 40 years ago.

The IEEE's involvement in the Huawei/BIS issue should be understood in the historical context of the U.S. government's continuous attempt to draw professional societies into positions of agency. Once again, the IEEE and Computer Society membership, in the person of George Davida and anonymous contemporaries, has performed in bravura fashion by carefully guiding our societies to the right side of history. This is as it should be. However, societies should take a much more proactive stance against being drawn into these issues. Professional societies and governments have very distinct missions, and these should not be confused. Although there may be disagreement over what the proper role of government should be (an issue I take no position on here), there should be little or no disagreement over the proper role of our professional societies. The recent American Psychological Association debacle[6] should give us all pause that the membership needs to take a far more active role in the shaping and implementation of policy by professional societies.

In this age of tribalism and weaponized disinformation, we must be careful to clearly articulate our positions. I am not denying that a state may have national security objectives that may be served by, or strongly overlap, academic and professional research interests—whether in computing (as in cryptography, cybersecurity, and cyber warfare), the physical sciences (biological, chemical, and nuclear weaponry), the social sciences (psychological operations and social engineering), and so on. However, we may willingly admit the fundamental responsibility of a government to protect its citizens' security without conceding anything along the lines of censorship and the corruption of professional organizations.

It is wise to remain agnostic regarding whether the current national security policies, strategies, and tactics are adequate to this challenge because they are protected by veils of secrecy and are immune from public scrutiny and accountability. That said, I argue here that government censorship of such research is inconsistent with constitutional safeguards and should not be tolerated—by us or our professional representatives. Edward Shils observed that a balance must be struck between publicity, privacy, and secrecy, and this balance must not include the corruption of the scientific enterprise or subversion of democratic principles. There are mechanisms, such as nondisclosure agreements and security clearances, that may be used to protect governmental interests. Censorship and deceit are unnecessary.

To confuse the separate responsibilities of government and professional societies (or allow them to be coopted by one another) creates a deformation of the body politic from which democracy cannot easily recover. Fortunately for all of us, the IEEE and the IEEE Computer Society have, in these cases and albeit reluctantly at times, avoided being drawn into any such deformation by a membership animated to speak out on the issues. For that, we should all be most appreciative. C

REFERENCES

1. P. Bump, "The NSA lost a free speech lawsuit (involving a T-shirt)," *The Atlantic*, Feb. 18, 2014. [Online]. Available: https://www.theatlantic.com/politics/archive/2014/02/nsa-lost-free-speech-lawsuit-involving-t-shirt/358230/
2. J. Whitehead, "Free speech, Facebook and the NSA: The good, the bad and the ugly," *HuffPost*, June 4, 2015. [Online]. Available: https://www.huffpost.com/entry/free-speech-facebook-and_b_7497064
3. J. Bamford, *The Puzzle Palace*. Baltimore, MD: Penguin Books, 1983.
4. M. Talev, N. Wadhams, and J. Jacobs, "Trump says he'll allow China's Huawei to buy from U.S. suppliers," *Bloomberg*, June 29, 2019. [Online]. Available: https://www.bloomberg.com/news/articles/2019-06-29/trump-says-he-ll-allow-china-s-huawei-to-buy-from-u-s-suppliers
5. H. Berghel, "The intimidation factor: How a surveillance state can affect what you read in professional publications," *Computer*, vol. 46, no. 12, pp. 91–95, Dec. 2013. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6689262
6. H. Berghel, "What price Gonzo ethics?" *IEEE Computer*, vol. 48, no. 12, pp. 88–93, Dec. 2015. doi: 10.1109/MC.2015.355. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7367985

7. H. Berghel, "Codes of ethics in a post-truth world," *IEEE Computer*, vol. 52, pp. 76–80, Mar. 2019. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8677356
8. S. Sanders, "Data privacy: What Washington doesn't want you to know," *Reason*, Jan. 1981. [Online]. Available: https://reason.com/1981/01/01/data-privacy-what-washington-d
9. H. Berghel, "Legislating technology (badly)," *IEEE Computer*, vol. 48, pp. 72–78, Oct. 2015. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7310956
10. "Scientists warned of U.S. curbs," *NY Times*, Jan. 8, 1982. [Online]. Available: https://www.nytimes.com/1982/01/08/us/scientists-warned-of-us-curbs.html
11. P. Zimmerman, "Why do you need PGP," *Ethical Spectacle*, July 1995. [Online]. Available: http://www.spectacle.org/795/byzim.html
12. V. Sussman, "Lost in Kafka territory: The fed go after a man who hoped to protect privacy rights," *U.S. News and World Report*, Mar. 26, 1995. [Online]. Available: https://web.archive.org/web/20130616165334/http://www.usnews.com/usnews/news/articles/950403/archive_010975.htm
13. S. Ranger, "Defending the last missing pixels: Phil Zimmermann speaks out on encryption, privacy and avoiding the surveillance state," *TechRepublic*, June 23, 2015. [Online]. Available: https://www.techrepublic.com/article/defending-the-last-missing-pixels-phil-zimmermann/
14. p. Zimmerman, "The Zimmerman case," *Ethical Spectacle*, July 1995. [Online]. Available: http://www.spectacle.org/795/zimm.html
15. J. Bartlett, "Cypherpunks write code," *American Scientist*, Mar.–Apr. 2016. [Online]. Available: https://www.americanscientist.org/article/cypherpunks-write-code
16. J. Gilmore, "DES (data encryption standard) review at Stanford University," Dec. 21, 2015. [Online]. Available: http://www.toad.com/des-stanford-meeting.html
17. M. Hellman, "The wisdom of foolishness: Stanford Engineering Hero Lecture," Jan. 13, 2013. [Online]. Available: https://www.youtube.com/watch?v=XDgLDsUU7og
18. B. Orlin, "The professor vs. the NSA," Heidelberg Laureate Forum, *Math with Bad Drawings*, Oct. 11, 2017. [Online]. Available: https://mathwithbaddrawings.com/2017/10/11/the-professor-vs-the-nsa/
19. A. Zegart, "The NSA confronts a problem of its own making," *The Atlantic*, June 29, 2017. [Online]. Available: https://www.theatlantic.com/international/archive/2017/06/nsa-wannacry-eternal-blue/532146/
20. A. Greenberg, "The Shadow Brokers mess is what happens when the NSA hoards zero-days," *Wired*, Aug. 17, 2016. [Online]. Available: https://www.wired.com/2016/08/shadow-brokers-mess-happens-nsa-hoards-zero-days/
21. D. P. Moynihan, *Secrecy*, 1st ed. New Haven, CT: Yale Univ. Press, 1998.
22. "Report of the Commission on Protecting and Reducing Government Secrecy," S. Doc. 105-2, Washington, D.C.: U.S. Govt. Printing Office, Dec. 31, 1997.
23. E. Shils, *The Torment of Secrecy: The Background and Consequences of American Security Policies*. Chicago, IL: Univ. of Chicago Press, 1956.
24. S. Horton, *Lords of Secrecy: The National Security Elite and America's Stealth Warfare*. New York: Bold Type Books, 2015.
25. G. McGraw, "Silver bullet talks with Martin Hellman," *IEEE Security Privacy*, vol. 14, no. 4, pp. 7–11, July–Aug. 2016.
26. "New York Times Co. v. United States," U.S. Supreme Court, 403 U.S. 713, 1971. [Online]. Available: https://supreme.justia.com/cases/federal/us/403/713/
27. F. Weingarten, "Testimony of before the U.S. Copyright Office on the need for exemptions from the anticircumvention provisions of the Digital Millennium Copyright Act," May 19, 2000. [Online]. Available: https://www.copyright.gov/1201/hearings/2000/fred_weingarten.pdf
28. E. Geller, "Trump officials weigh encryption crackdown," *Politico*, June 27, 2019. [Online]. Available: https://www.politico.com/story/2019/06/27/trump-officials-weigh-encryption-crackdown-1385306
29. Z. Doffman, "U.S. may outlaw messaging encryption used by WhatsApp, iMessage and others, report claims," *Forbes*, June 29, 2019. [Online]. Available: https://www.forbes.com/sites/zakdoffman/2019/06/29/u-s-may-outlaw-uncrackable-end-to-end-encrypted-messaging-report-claims/#7fc3fad06c87
30. U.S. Department of Commerce, Bureau of Industry and Security. [Online]. Available: https://www.commerce.gov/bureaus-and-offices/bis
31. U.S. Department of Commerce, "Department of Commerce issues limited exemptions on Huawei products," May 20, 2019. [Online]. https://www.commerce.gov/news/press-releases/2019/05/department-commerce-issues-limited-exemptions-huawei-products.
32. P. Zimmermann, "Frequently asked question." Accessed on: June 1, 2019. [Online]. https://www.philzimmermann.com/EN/faq/index.html.

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