Hey, You've Got to Hide Your Work Away

Debate is simmering over how and when to publish sensitive data

Not long after letters laced with anthrax spores killed five Americans in September 2001, a research team led by genome scientist Harold "Skip" Garner came up with an idea for probing such crimes. But the solution gave him pause. During a study that used new gene technologies to analyze several of the world's deadliest pathogens, the researchers realized that a unique genetic "barcode" could be discreetly inserted into laboratory strains, potentially enabling forensic scientists to track a bioweapon or escaped pathogen back to its source. It was just the kind of tagging that could have helped investigators identify the source of the weaponized anthrax spores tucked into the deadly letters, says Garner, now with the Virginia Bioinformatics Institute at the Virginia Polytechnic Institute and State University in Blacksburg. But publishing the trick might also aid evildoers, he realized. "It was information that might be misused, to figure out how to evade detection," Garner recalled recently. "We had to ask: 'Is it wise to widely share this?' "

That question is confronting many scientists these days. Every research field has findings so sensitive that scientists can spend countless hours fretting over when, where, and how to publish them—or whether to share them at all. For microbiologists and chemists, it might be a technique that could be misused to create a terrifying weapon. For biomedical and social scientists, huge databases of personal health and behavioral information pose threats to privacy. Archaeologists and wildlife biologists worry about pinpointing some study sites, fearful they could guide looters and poachers to priceless artifacts or vulnerable species.

It's not a new conundrum. Academic researchers have long struggled to balance an ethos of openness with demands for secrecy. Most famously, perhaps, U.S. nuclear scientists in the late 1930s and early 1940s kept mum about findings that they worried might give Nazi Germany clues to building an atom bomb.

Today's struggles over sensitive data may have lower stakes, but they are increasingly pervasive and complex. More scientists are engaged in work that requires secrecy in the name of protecting national security, intellectual property, and confidentiality. And researchers may not get to make the call; government regulators, corporate lawyers, and even ethicists are demanding a bigger say in deciding when to let information loose and when to lock it up. Ironically, some agencies publish classified journals for scientists with security clearances to have a place to share peer-reviewed secrets (see sidebar, p. 71).

Such trends are forcing scientists to rethink how they publish papers and agencies to reconsider which studies to fund. And they are helping spur the growth of new bureaucracies designed to avoid the unintentional release of sensitive data—or even prevent such data's creation in the first place. Whether such controls will ultimately help or harm science and society, however, is the subject of vigorous debate. "Open communication among scientists is critical to the good that science can do, but concerns about the misuse of information are testing that ideal," says ethicist and molecular biologist Kathleen Kolakovich Eggleson of the University of Notre Dame in Indiana. And with the Internet making it nearly impossible to recapture sensitive data once they have escaped, she says, "it's an issue that's just going to become even more problematic."

Rude awakening

For some scientists, the clamor that can arise around sensitive data comes as a shock. Influenza researchers, for instance, were largely caught off guard in 2011 when a global, yearlong controversy engulfed efforts by two teams to publish papers, in *Science* and *Nature*, which showed how to engineer the dangerous H5N1 influenza virus, which normally infects birds, so that it can also move between mammals (*Science*, 6 April 2012, p. 19). Officials in the U.S. government—which funded the studies—became concerned that a mutant virus

ILLUSTRATION: DAVID PLUNKERT

could escape from a lab and cause a human pandemic, or that revealing details about the research could inadvertently aid terrorists seeking a bioweapon. They asked the National Science Advisory Board for Biosecurity, set up after the 2001 anthrax attacks, to review the H5N1 studies. It initially recommended that the papers be published only if journal editors deleted key methodological details and shared them only with "responsible" scientists. In the end, however, such selective censorship proved both practically and legally impossible, and a divided advisory board ultimately supported full publication of both studies, which appeared in print last year.

The episode has left a mark on science. For instance, it prompted the government of the Netherlands to take the unusual step of requiring researchers there to obtain an export permit before sending their final manuscript to *Science* in the United States—a precedent for government oversight of data sharing that worries some scientists. And it prompted the U.S. National Institutes of Health (NIH), the world's biggest biomedical science funder, to impose extensive new rules. NIH-funded researchers and universities now must undertake special reviews of proposed studies that involve H5N1 and more than a dozen other risky biological agents and toxins. The goal: to identify experiments that might produce sensitive "dual use" findings that could be used for good and evil—and force alterations or even stop them before they begin. If NIH were to fund a study that meets the dual use definition, the agency announced in August, researchers must create "risk mitigation" plans that include strategies to control sharing sensitive results. And they must allow NIH to see manuscripts and abstracts at least 10 days prior to submission to a journal or meeting.

Such prior review requirements are already common in academic studies funded by industry, which is keen to patent profitable ideas before they become public, and military agencies, which aren't eager to aid adversaries. Still, some researchers fear that NIH's adoption of prior review for a new swath of academic science could signal a creeping expansion of bureaucratic controls. Journal editors and legal specialists say it's not clear whether the U.S. government can legally block publication of NIH-funded data unless it takes the radical step of classifying them as secret.

Such questions may not be resolved for some time. In the short term, the new rules are expected to affect just a handful of studies. Editors of major scientific journals say that they rarely see truly sensitive manuscripts. A 2008 study, for instance, found that just six of 16,000 manuscripts submitted to the 11 journals published by the American Society for Microbiology over a 5-year period raised dual use concerns. Just two weren't published because the authors wanted to withhold methodological details.

A dearth of worrisome manuscripts doesn't mean people aren't making worrisome discoveries; researchers may simply be sitting on sensitive results. In a paper to be published later this year by the *Saint Louis University Journal of Health Law & Policy*, David Franz, former commander of the U.S. Army Medical Research Institute of Infectious Diseases in Frederick, Maryland, recalls that, in the 1990s, scientists there unintentionally created a virus strain that was resistant to a potential treatment. After a discussion, "we decided to put the entire experiment into the autoclave," Franz tells *Science*. "That was it. We didn't hear anyone say: 'Wow, we could get a paper in *Science* or *Nature*.' "

Garner took a similarly cautious approach with his barcoding technology. "We wrote up a white paper for some of the government agencies, but didn't distribute it widely," he says. "Seemed better that way."

Censorship or discretion?

In other fields, scientists are learning that they may give away sensitive data without being aware they'd let it slip. Archaeologists have posted pictures of new finds on websites only to discover that savvy thieves have tapped metadata digitally attached to images to discover location information—and then looted the site. Conservation biologists often refrain from saying exactly where they've spotted a rare species, for fear an overzealous collector or landowner will hunt it down. Genome researchers and social scientists have been stung by computer wizards who have shown that they can take databases that supposedly have been stripped of information allowing the identification of individuals and "re-identify" study participants, violating privacy rules. In theory, such techniques could reveal a trove of problematic information, such as embarrassing Web surfing habits, stigmatizing mental health issues, or genetic traits that could affect employment or insurance.

As plant biologist Rodrigo Gutiérrez of the Catholic University of Chile in Santiago puts it: "We are gaining the capacity to generate lots of sensitive information, but not necessarily the capacity to handle it appropriately."

–DAVID MALAKOFF

Cloak-and-Dagger Publishing

A hot new journal debuted last month, but you can't read it—or publish in it—unless you have a security clearance from the U.S. government. The *Journal of Sensitive Cyber Research and Engineering* (*JSCoRE*) is the newest addition to the shadowy shelf of "dark," or classified, journals that aim to solve a thorny problem: how to rigorously peer review and share sensitive government-funded findings that officials don't want sent to regular journals.

"Even though the community of researchers doing sensitive work has the same needs as those doing unrestricted research, the absence of a peer-reviewed publication … impedes the quality and progression of sensitive science," wrote *JSCoRE* co-editor William "Brad" Martin of the U.S. National Security Agency and colleagues in a poster on the journal's origins that they presented at a meeting last year. To help researchers in the booming field leap that obstacle, the poster promises that *JSCoRE* will "feature an editorial board consisting of cyber luminaries from inside and outside of government" and "qualified peer reviewers."

JSCoRE may reside where few can lay eyes on it, but it has plenty of company. Worldwide, intelligence services and military forces have long published secret journals that often touch on technical topics. The demand for restricted outlets is bound to grow as governments classify more information; the United States alone has dozens of categories of controlled information, including "top secret," "for official use only," and "sensitive but unclassified." But going dark doesn't mean keeping the general public entirely in the dark: *JSCoRE* has asked authors to provide titles and abstracts that don't have to be kept secret, so the journal can appear in public indexes.

–D. M.