frontiers in Bioengineering and Biotechnology

PERSPECTIVE
published: 25 February 2019
doi: 10.3389/fbioe.2019.00021

National and Transnational Security Implications of Asymmetric Access to and Use of Biological Data

Kavita M. Berger[1]* *and Phyllis A. Schneck*[2]

[1] Gryphon Scientific, LLC, Takoma Park, MD, United States, [2] Promontory Financial Group, an IBM Company, Washington, DC, United States

Biology and biotechnology have changed dramatically during the past 20 years, in part because of increases in computational capabilities and use of engineering principles to study biology. The advances in supercomputing, data storage capacity, and cloud platforms enable scientists throughout the world to generate, analyze, share, and store vast amounts of data, some of which are biological and much of which may be used to understand the human condition, agricultural systems, evolution, and environmental ecosystems. These advances and applications have enabled: (1) the emergence of data science, which involves the development of new algorithms to analyze and visualize data; and (2) the use of engineering approaches to manipulate or create new biological organisms that have specific functions, such as production of industrial chemical precursors and development of environmental bio-based sensors. Several biological sciences fields harness the capabilities of computer, data, and engineering sciences, including synthetic biology, precision medicine, precision agriculture, and systems biology. These advances and applications are not limited to one country. This capability has economic and physical consequences, but is vulnerable to unauthorized intervention. Healthcare and genomic information of patients, information about pharmaceutical and biotechnology products in development, and results of scientific research have been stolen by state and non-state actors through infiltration of databases and computer systems containing this information. Countries have developed their own policies for governing data generation, access, and sharing with foreign entities, resulting in asymmetry of data sharing. This paper describes security implications of asymmetric access to and use of biological data.

Keywords: biotechnology, cybersecurity, information security, data vulnerability, biological data, biosecurity, data access, data protection

OPEN ACCESS

Edited by:
Randall Steven Murch, Virginia Tech, United States

Reviewed by:
Segaran P. Pillai, United States Department of Homeland Security, United States
Jacqueline Fletcher, Oklahoma State University, United States

***Correspondence:**
Kavita M. Berger
kberger@gryphonscientific.com

Specialty section:
This article was submitted to Biosafety and Biosecurity, a section of the journal Frontiers in Bioengineering and Biotechnology

Received: *29 November 2018*
Accepted: *29 January 2019*
Published: *25 February 2019*

Citation:
Berger KM and Schneck PA (2019) National and Transnational Security Implications of Asymmetric Access to and Use of Biological Data. Front. Bioeng. Biotechnol. 7:21. doi: 10.3389/fbioe.2019.00021

INTRODUCTION

Advances in computer science, engineering, and data science have changed research, development, and application of biology and biotechnology in the United States and internationally. Examples of changes include: (a) increased reliance on internet connectivity for research and laboratory operations (Accenture, 2015; Bajema et al., 2018; Olena, 2018); (b) increased use of automation in life-science laboratories (Chapman, 2003); (c) application of the "design-build-test" paradigm to create new biological organisms (Agapakis, 2014; Carbonell et al., 2018); (d) increased generation, analyses, and computational modeling of information about biological systems, cells,

and molecules (Thurow et al., 2004; Walpole et al., 2013); (e) treatment of organisms and DNA as materials rather than phenomena to study (Service, 2017; Anderson et al., 2018; Patel, 2018); and (f) new funders such as venture capital, crowdfunding platforms, and foreign companies and governments (Von Krogh et al., 2012; Cha, 2015; Mervis, 2017). These changes have transformed the scientific, agricultural, and health communities' ability to understand and manipulate the world around them. In addition, the changes have enabled an influx of new practitioners and problem-solvers into biology, providing opportunities for education and research all over the world.

Biotechnology harnesses the capabilities of computer, data, and engineering sciences to establish and advance new fields such as synthetic biology, precision medicine, precision agriculture, and systems biology. Cloud-based platforms and open source, easy-to-use software enable scientists from anywhere in the world to use advanced data analytics in their studies. The software and hardware emerging from these fields improve our collective understanding of molecular and systems-level genetics, new drug therapies for longer and better quality of life, and design of novel and/or unnatural organisms. Critical to these pursuits is the sharing of research results and underlying data, without which societal decision-making about human, animal, plant, and environmental health cannot be realized fully. However, during the past two decades, concerns about data sharing have been raised, resulting in the issuance of international, regional, and national-level policies governing access to different types of data, including biological data. In addition, the platforms through which data are stored, transported, and analyzed may be vulnerable to unauthorized acquisition of information by malicious actors, which could lead to significant economic and physical harms to the health, safety, and security of a population. Although not considered "dual use life sciences research of concern" U. S. Government, 2012, 2014), the potential for both benefit and risk to humanity meets the spirit of the dual use concept (National Research Council, 2004). Given the significant benefits afforded by data sharing and analysis, this paper highlights current data protection policies, potential risks of data exploitation by malicious actors, and potential strategies to mitigate those risks and promote rapid recovery in biotechnology fields that are breached.

The interconnectedness between the digital and biological worlds can be exploited by state actors, malicious nonstate actors, and hackers through a variety of means, resulting in harmful consequences from potential theft of information, promulgation of incorrect information, and/or disruption of activities (Lord and Forbes Technology Council, 2017; Souza, 2018; Ward, 2018). For example, theft of proprietary information from a pharmaceutical or biotechnology company may reveal trade secrets and allow competitors to develop superior products and/or bring existing products to market more quickly (Friedman, 2013), stifling innovation in the global commercial market and allowing adversaries to create harmful, untested therapies. Another example is theft of hundreds of millions of electronic healthcare records, the uses of which are not clear (Bogle, 2018; Cohen, 2018; Healthare IT News Staff, 2018; Huang and Steger, 2018; Keown, 2018). Although unauthorized access to protected data may be aided by technical vulnerabilities in networked computer systems, poor security practices, insider threats in academia, industry, and health facilities, and legal business dealings also can enable adversary access to such data (Lynch, 2017; Rappeport, 2018; South China Morning Post, 2018; Zhu, 2018). For examples, more than half of all data breaches at healthcare facilities are caused by healthcare personnel errors, a quarter of which resulted in unauthorized access to or disclosure of patient records through sharing of unencrypted information, sending information to the wrong patients, and accessing the data without authorization (Bai et al., 2017; Michigan State University, 2018). In addition, the Federal Bureau of Investigation (FBI) has raised national security concerns about foreign access to genomic data of U.S. citizens through legitimate scientific collaboration, funding of scientific research, investment in genomic sequencing companies [e.g., China-based WuXi Healthcare Ventures investment in the U.S.-based 23andMe (Biospace, 2015; Mui, 2016)], and purchase of companies (e.g., Complete Genomics) (Baker, 2012; GenomeWeb, 2012). As vulnerabilities are created through scientific advances, such as the use of machine learning algorithms to trick fingerprint authentication systems, new risks are identified (Bontrager et al., 2018; Nyu Tandon School of Engineering, 2018). Some of these concerns have resulted in the passage of the 2018 Foreign Investment Risk Review Modernization Act, which has initiated reform of the U.S. Government process for evaluating foreign investment in U.S. entities and export control of emerging technologies (Rappeport, 2018; U.S. Congress, 2018). Yet, these policy activities largely are reactive, rather than proactive.

CURRENT APPROACHES FOR PROTECTING DATA

Preventing accidental and deliberate risks typically involves the use of cyber and information security systems that include technological and behavioral solutions. Protection of laboratory control systems, computer networks, and databases often involves the use of technological solutions. However, some risks are addressed better through training of personnel to recognize and report phishing attempts, ensure sensitive information is encrypted, and prevent unauthorized individuals from gaining access to sensitive data, databases, and computer networks. To enhance security, policies for promulgating these practices for specific materials and information have been issued. For example, the U.S. Biological Select Agents and Toxins Regulations include guidance for network security to prevent failure of laboratories, equipment, and access controls to facilities and data (Federal Select Agent Program, 2017). In addition, the U.S. has policies for protecting individual privacy, several of which were described in a 2014 report sponsored by the White House (Podesta et al., 2014). However, error, carelessness, or negligence by personnel can counteract the benefits afforded by security measures and may lead to devastating consequences if biological data and materials are involved.

Although policies for protecting biological data from cyberattack are limited, policies that govern data access and sharing are prevalent. These top-down, data access policies intend to protect individual rights and/or prevent sharing or distribution of data, including biological data. Examples of recent policies include: (a) the 2018 update of the European Union General Data Protection Regulation (European Commission, 2018), which strengthened the European Union's rules for protecting personal data of individuals, in part by giving its citizens "more control over their personal data;" (b) the 2018 Chinese Personal Information Security Specification, which is one system under the Chinese Cybersecurity law, involves the "collection, storage, use, sharing, transfer, and disclosure of personal information," and enables companies operating in China to access data to "not hamper the development of fields like AI" (Sacks, 2018); (c) the 2018 General Data Protection Law in Brazil, which provides a framework for the use of personal data in Brazil (Soares, 2018); and (d) the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), which promotes the protection of privacy and security of patient health information in the United States (Department of Health and Human Services, 2017). At the same time, the U.S. has issued policies governing data generation, access, and sharing to promote information-sharing and transparency of government-sponsored research (Noorden, 2013). Internationally, the Nagoya Protocol of the Convention on Biodiversity[1] promotes governance on access to and fair, equitable sharing of the benefits from the use of non-human biological data. However, questions exist about whether the Nagoya Protocol focuses more on biological samples that provide genetic information or the genetic information itself, which ultimately affects national-level efforts for codifying the international agreement (Dos et al., 2018). Despite these activities, protection of some data, such as personal health data, may not extend beyond a country's borders and may apply only to data collected by certain entities. Furthermore, data protection polices do not extend to information that already has been stolen. Taken together, these national, regional, and international level policies for data protection may not prevent the inappropriate or unauthorized acquisition of data to different actors, the consequences of which are unclear for biotechnology data.

VULNERABILITY OF BIOTECHNOLOGY DATA

The primary challenges in identifying, assessing, and mitigating security vulnerabilities of biotechnology data are understanding: (a) how the data may be exploited by adversaries and what consequences result from this exploitation; and (2) what potential negative effects may arise from digitalization of biotechnology and advanced computation of biological data (Bajema et al., 2018). The term "biotechnology" refers to the exploitation of biological processes for industrial and scientific purposes, and includes genetic manipulation of microbes, plants, animals, human cells, nucleic acids (the building blocks of genomes), and proteins (the functional units in cells). This definition is expanded further to include generation, incorporation, and use of digital forms of biological data. These biological data may be available online through databases, such as the U.S. National Center for Biotechnology Information's GenBank[2], or generated in a laboratory and stored, shared, and/or analyzed locally or remotely (via online and/or cloud-based software). By attempting to answer the questions posed above, specific risks associated with the legal and illegal acquisition of biological data may be identified and mitigated.

Although extraordinary advances in computing power are enabling unprecedented scientific discoveries, its application to biology and healthcare is increasing without effective protection from the risks of adversary acquisition or accidental misuse of information. Scientific data that is generated in basic and applied research laboratories in academia, non-profit research organizations, service providers, and some industry research facilities may be considered fundamental research destined for publication and public benefit. These data are not necessarily sensitive, but they do represent the results of significant investment by governments, industry, investors, and philanthropic organizations. Therefore, theft or large-scale acquisition of these data may have adverse economic consequences to the organization, field, or nation, especially if acquisition was directed by adversarial nation-states to gain competitive advantage in a given sector (Blair and Huntsman, 2013). As previously described, databases that store sensitive and/or non-sensitive biological data have been infiltrated by external actors and accessed by unauthorized individuals. Although measures to protect data have been implemented in several institutions, cyber and information security policies, practices, and compliance vary across biotechnology sectors, location, and organization type (e.g., academia, industry). Although implementation of cyber, information, and data security in biological facilities can help to minimize the potential for deliberate or accidental release of protected biological data, these measures are insufficient on their own (Press, 2018).

Furthermore, the increasing size and volume of the datasets, and the complexity of analytic technologies has led many scientists to rely on cloud-based platforms to store, transfer, and analyze data. These platforms and technologies, including online analysis software and applications, often do not prevent unauthorized access to data or ensure software fidelity. Although mitigating specific vulnerabilities may be possible on an individual platform or technology level, implementing protections across the various data generation, analysis, transfer, and storage platforms currently in use in academia, industry, government laboratories, and healthcare facilities is challenging. Countering these risks requires the identification of consequences that are of particular concern to public safety

[1]Convention on Biodiversity. About the Nagoya Protocol. Available online at: https://www.cbd.int/abs/about/ (Accessed November 23, 2018).

[2]National Center for Biotechnology Information. GenBank. Available online at: https://www.ncbi.nlm.nih.gov/genbank/ (Accessed November 23, 2018).

and national security, evaluation of vulnerabilities that may enable the realization of these consequences, and identification of measures to address these vulnerabilities.

POSSIBLE PREVENTION AND MITIGATION APPROACHES

Modern cyber and information security reflects the risks experienced as the internet has grown and diversified, and as the capabilities for and speed of storing, processing, and transporting information have increased exponentially (Denning and Lewis, 2017). The internet was built without a priority on the protection of data whether "at rest" (i.e., stored data) or "in motion" (i.e., data in transit) (Dauch et al., 2009; Inap, 2013). Current strategies for addressing cyber risks focus on remediation through regulation, organizational support, and actions taken by data owners and consumers in the form of encryption technologies, access control measures, awareness-raising campaigns, risk assessment, blocking, limiting publication of sensitive information, and other similar practices. The challenge is understanding how these measures are to be applied to biotechnology data, how to balance the cost of implementation with the consequences if left unprotected, and what vulnerabilities cannot be mitigated using commercial products.

Often the entities that assess their cyber vulnerabilities and invest in cyber and information security measures are compelled to do so because of regulation and fiscal responsibility (McDonald, 2017). However, unlike financial information, biotechnology data is regulated in some countries, but not others. For example, China issued a recent policy requiring a domestic collaborator and Ministry-level approval for research involving genomic data of Chinese citizens and/or biological samples obtained in China to prevent exploitation of these data and samples (Tuzman, 2018). This and similar policies raise questions about their intended and unintended effects to nations, to the scientific community, and to international security mainly because the policies that may benefit one country could harm another. These harms may reveal new types of risks associated with the acquisition and use of data to manipulate biological systems. These risks may be perpetrated by different actors; affect sector and country economies, commercial biotechnology, and pharmaceutical markets domestically and internationally; and alter global strategic power dynamics.

The risks associated with biotechnology data do not conform to traditional biosecurity concerns, which focus primarily on risks to human health or the food and agriculture economy. These risks involve multiple domains, sectors, and nations resulting in outcomes such as shifting of balance of power of nations at the international level, which could have downstream effects on areas that overlap with biosecurity interests (e.g., biosafety and biosecurity, biothreat reduction, and global health security). Strategies for bridging the biological, cyber, information, and data security include: (a) collaboration between the biological and cybersecurity communities; (b) end-to-end risk assessments; (c) data-specific risk and vulnerability assessments; and (d) application of the NIST Cybersecurity Framework for protecting biological data.

Formal collaboration between the biotechnology and biological, information, data, and cyber security communities would enhance efforts toward identification of risks and vulnerabilities associated with data management, provenance, and integrity, and risk mitigation strategies. Technologies are readily available to protect data, but their use must be harmonized worldwide, because protecting data in one database is ineffective if another database remains vulnerable to external threats. Furthermore, organizations may evade regulatory requirements and industry standards in protecting data because of perceived lack of cost savings for implementing cybersecurity measures or lack of awareness of the risks, which could lead to investor, intruder, or adversary access to sensitive information that may be stored in databases or transferred between computers. These vulnerabilities may be exacerbated by limitations of national laws to other sovereign states, and differences in interpretation of the types of data included in the scope of existing laws. **Given these potential vulnerabilities, the cybersecurity and biotechnology communities must engage to create best practices and processes to protect data and mitigate risk while reaping the benefits of computing technology applications to biotechnology.**

End-to-end assessments of the data storage, processing, and transport pipeline can identify outstanding vulnerabilities and technical gaps that may be addressed with currently available cyber, information, and data security solutions. This process would enable identification of gaps for which these measures are insufficient and of institutions that are responsible for implementing controls. Without this type of assessment, vulnerabilities may exist along the pipeline without its users' knowledge. A lack of rigorous analysis makes biological data vulnerable to acquisition or alteration by witting adversaries, potentially resulting in theft of intellectual property for commercial gain, foreign government acquisition of genomic data from large portions of a population for undefined purpose or compromise of software and data integrity. At least one country promotes acquisition of data though legitimate commercial practices (e.g., providing sequencing services to customers; partnering with academia, independent research institutions, and universities; and foreign investment), talent promotion programs (Capaccio, 2018; Nature Jobs, 2018), and theft of data (Riley and Walcott, 2015; Dilanian, 2018; Kaiser and Malakoff, 2018; Wilber, 2018). The FBI has expressed concerns about the theft of U.S. genomics and health information through cyberattacks and foreign investment in the U.S. biotechnology industry (You, 2017). The FBI argues that acquisition of this information can give adversaries an unfair advantage in the international pharmaceutical or biotechnology marketplace. Others have expressed concern about questionable use of genetic information that countries obtain from their own citizens or from other countries' citizens (Human Rights Watch, 2017; Lynch, 2017; Pauwels and Vidyarthi, 2017). **These risks could be addressed by conducting an end-to-end risk assessment of the software**

and equipment involved in the data pipeline within individual organizations, between organizations, and across countries.

Defining the consequences of greatest concern to national security is an initial step toward assessing the risks and vulnerabilities of the information itself and data-specific risk mitigation strategies. Evaluating these risks enables the identification of content-specific approaches for detecting and countering exploitation of vulnerabilities by insider and external actors. Without these assessments, only generic cyber and information security measures will be implemented. However, these measures are insufficient to counter adversaries who are intent on acquiring data through a variety of technical, social engineering, or other means. Given this reality, rapid detection and resilience (i.e., rapid recovery after a breach) are critical for reaping the benefits and minimizing the vulnerabilities of advanced electronic computation and mass connectivity. In 2014, the White House explored technology needs for protecting the security and privacy of exposed data, including healthcare data (Executive Office of the President, 2014; President's Council of Advisors on Science Technology, 2014). But, these studies did not define consequences of concern related to the unauthorized acquisition of vast amounts of biological data, effectively limiting the identification of data-specific or process-specific prevention measures. **Therefore, risk assessments of specific types of data are equally as important to conduct as analyses of vulnerabilities of laboratory control systems, data management platforms, and computer networks.**

Application of the National Institute of Standards and Technology (NIST) Cybersecurity Framework to all systems of storage, processing and transport of biological data would help explore where, how, and by whom data is processed with the goal of protecting valuable scientific and health information (National Institute of Standards Technology, 2018). The NIST framework involves a collaboration of private sector and government cybersecurity experts that seek to apply the five principles of data protection (i.e., identify, protect, detect, respond, and recover) to systems, including those on which biological data are generated, processed and transported. The framework could augment existing or newly-implemented efforts of vulnerability detection and mitigation, thus decreasing unauthorized exposure of sensitive data. The NIST framework is a widely accepted paradigm for cyber risk management and best practices (Department of Homeland Security, 2018; Lohrmann, 2018; Roncevich, 2018). In the U.S., this framework has been used in regulatory dialogues to demonstrate rigor toward cybersecurity in sectors for which such requirements are not well-documented in law. **Application of the NIST framework to biotechnology can enhance data protection and a focus on rapid detection of nefarious activity and resiliency after an attack.**

These suggestions describe various approaches toward protecting biological data from unauthorized acquisition and use, enhancing efforts to preserve data integrity and provenance, and enabling future benefit of biotechnological advances.

AUTHOR CONTRIBUTIONS

KB and PS contributed equally to this manuscript. The concepts, conclusions, and recommendations were generated jointly by the authors and built on their respective expertise in the biological sciences and biosecurity, and computer science and cybersecurity.

REFERENCES

Accenture (ed). (2015). *The Future of Applications in Life Sciences: New application Strategies to Unlock the Digital Opportunity.* A.L. Sciences.

Agapakis, C. M. (2014). Designing synthetic biology. *ACS Synth. Biol.* 3, 121–128. doi: 10.1021/sb4001068

Anderson, L. A., Islam, M. A., and Prather, K. L. J. (2018). Synthetic biology strategies for improving microbial synthesis of "green" biopolymers. *J. Biol. Chem.* 293, 5053–5061. doi: 10.1074/jbc.TM117.000368

Bai, G., Jiang, J. X., and Flasher, R. (2017). Hospital risk of data breaches. *JAMA Intern. Med.* 177, 878–880. doi: 10.1001/jamainternmed.2017.0336

Bajema, N. E., Dieuliis, D., Lutes, C., and Lim, Y.-B. (2018). "The digitalization of biology: understanding the new risks and implecations for governance," in *Emergence and Convergence,* ed National Defense University (Washington, DC: National Defense University), 2–3, 7–12.

Baker, M. (2012). China buys US sequencing firm. *Nature* 489, 485–486. doi: 10.1038/489485a

Biospace (2015). *WuXi Healthcare Invests in US Genomics Testmaker 23andMe*. BioSpace. Available online at: https://www.biospace.com/article/releases/-b-wuxi-healthcare-b-invests-in-us-genomics-testmaker-23andme-/

Blair, D. C., and Huntsman, J. M. (2013). *The Report of the Commission on the Theft of American Intellectual Property*. ed T. I. Commission (The National Bureau of Asian Research).

Bogle, A. (2018). *Healthcare Data a Growing Target for Hackers, Cyberseucrity Experts Warn*. ABC News. Available online at: https://www.abc.net.au/news/science/2018-04-18/healthcare-target-for-hackers-experts-warn/9663304 (Accessed November 23, 2018).

Bontrager, P., Roy, A., Togelius, J., Memon, N., and Ross, A. (2018). DeepMasterPrints: generating masterprints for dictionary attacks via latent variable evolution. *arXiv*.

Capaccio, A. (2018). *U.S. Faces 'Unprecidented Threat' From China on Tech Takeover*. Bloomberg. Available online at: https://www.bloomberg.com/news/articles/2018-06-22/china-s-thousand-talents-called-key-in-seizing-u-s-expertise (Accessed November 23, 2018).

Carbonell, P., Jervis, A. J., Robinson, C. J., Yan, C., Dunstan, M., Swainston, N., et al. (2018). An automated design-build-test-learn pipeline for enhanced microbial production of fine chemicals. *Commun. Biol.* 1:66. doi: 10.1038/s42003-018-0076-9

Cha, A. E. (2015). Crowdfunding propels scientific research. *The Washington Post*.

Chapman, T. (2003). Lab automation and robotics: automation on the move. *Nature* 421, 665–666. doi: 10.1038/421665a

Cohen, J. (2018). *Massive Cyberhack by Iran Allegedly Stole Research from 320 Universities, Governments, and Companies*. Science. Available online at: https://www.sciencemag.org/news/2018/03/massive-cyber-hack-iran-allegedly-stole-research-320-universities-governments-and

Dauch, K., Hovak, A., and Nestler, R. (2009). "Information assurance using a defense in-depth strategy," in *Conference For Homeland Security, 2009 CATCH'09, Cybersecurity Applications and Technology* (Washington, DC), 267–272.

Denning, P. J., and Lewis, T. G. (2017). Exponential laws of computing growth. *Commun. ACM.* 60, 54–65. doi: 10.1145/2976758

Department of Health and Human Services (2017). *Summary of the HIPAA Security Rule.* Washington, DC. Available online at: https://www.hhs.gov/

hipaa/for-professionals/security/laws-regulations/index.html (Accessed November 23, 2018).

Department of Homeland Security (2018). *Using the Cybersecurity Framework*. Available online at: https://www.dhs.gov/using-cybersecurity-framework (Accessed January 24, 2019).

Dilanian, K. (2018). *China's Hackers Are Stealing Secrets From U.S. Firms Again, Experts Say*. NBC News. Available online at: https://www.nbcnews.com/news/china/china-s-hackers-are-stealing-secrets-u-s-firms-again-n917836 (Accessed January 27, 2019).

Dos, S. R. C., Koopmans, M. P., and Haringhuizen, G. B. (2018). Threats to timely sharing of pathogen sequence data. *Science* 362, 404–406. doi: 10.1126/science.aau5229

European Commission (2018). *2018 Reform of EU Data Protection Rules*. European Commission.

Executive Office of the President (2014). *Big Data: Seizing Opportunities, Preserving Values*. Washington, DC: White House.

Federal Select Agent Program (2017). *Information Systems Security Controls Guidance*. Atlanta, GA.

Friedman, A. A. (2013). *Cyber Theft of Competitive Data: Asking the Right Questions*. Brookings Institution.

GenomeWeb (2012). *Complete Genomics, BGI Agree to $117.6M Merger*. GenomeWeb. Available online at: https://www.genomeweb.com/sequencing/complete-genomics-bgi-agree-1176m-merger#.XEqIOFxKiUl (Accessed January 24, 2019).

Healthare IT News Staff (2018). *The Biggest Healthcare Data Breaches of 2018 (So Far)*. Healthcare IT News. Available online at: https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far (Accessed November 23, 2018).

Huang, E., and Steger, I. (2018). *China is Secretly Enrolling Military Scientists in Western Universities*. Defense One. Available online at: https://www.defenseone.com/threats/2018/10/china-secretly-enrolling-military-scientists-western-universities/152383/?oref=d-mostread (Accessed November 23, 2018).

Human Rights Watch (2017). *China: Minority Region Collects Data from Millions*. New York, NY: Human Rights Watch.

Inap (2013). *Data in Motion vs. Data at Rest*. Available online at: https://www.inap.com/blog/data-in-motion-vs-data-at-rest/ (Accessed January 24, 2019).

Kaiser, J., and Malakoff, D. (2018). NIH investigating whether U.S. scientists are sharing ideas with foreign governments. *Science*. doi: 10.1126/science.aav2343

Keown, A. (2018). *Second Scientist Pleads Guilty to Steeling GlaxoSmithKline Trade Secrets*. BioSpace. Available online at: https://www.biospace.com/article/-jc1n-second-scientist-pleads-guilty-to-stealing-glaxosmithkline-trade-secrets/ (Accessed November 23, 2018).

Lohrmann, D. (2018). *Why You Need the Cybersecurity Framework*. Government Technology.

Lord and Forbes Technology Council (2017). *The Real Threat Of Identity Theft Is In Your Medical Records, Not Credit Cards*. Forbes.

Lynch, D. J. (2017). *Biotechnology: the US-China Dispute over Genentic Data*. Financial Times. Available online at: https://www.ft.com/content/245a7c60-6880-11e7-9a66-93fb352ba1fe (Accessed November 23, 2018).

McDonald, K. (2017). *Private Sector's National Cybersecurity Strategy Contributions Lacking*. TechTarget. Available online at: https://searchcompliance.techtarget.com/opinion/Private-sectors-national-cybersecurity-strategy-contributions-lacking (Accessed January 24, 2019).

Mervis, J. (2017). Data check: U.S. government share of basic research funding falls below 50%. *Science*. doi: 10.1126/science.aal0890

Michigan State University (2018). *Healthcare Providers - Not Hackers - Leak More of Your Data*. EurekAlert!. Available online at: https://eurekalert.org/pub_releases/2018-11/msu-hp-111618.php (Accessed November 23, 2018).

Mui, Y. Q. (2016). *China's $9 Billion Effort to Beat the U.S. in Genetic Testing*. The Washington Post. Available online at: https://www.washingtonpost.com/news/wonk/wp/2016/12/30/chinas-9-billion-effort-to-beat-the-u-s-in-genetic-testing/?noredirect=on&utm_term=.3a83001d622d

National Institute of Standards and Technology (2018). *NIST Cybersecurity Framework*. ed D.O. Commerce. Washington, DC.

National Research Council (2004). *Biotechnology Research in an Age of Terrorism*. Washington, DC: National Academies Press.

Nature Jobs (2018). *China's Plan to Recruit Talented Researchers*. Career Guide. Available online at: https://www.nature.com/articles/d41586-018-\penalty-\@M00538-z

Noorden, R. V. (2013). *White House Announces New US Open-Access Policy*. Nature. Available online at: http://blogs.nature.com/news/2013/02/us-white-house-announces-open-access-policy.html (Accessed November 23, 2018).

Nyu Tandon School of Engineering (2018). *Machine Learning Masters the Fingerprint to Fool Biometric Systems*. PR Newswire. Available online at: https://www.prnewswire.com/news-releases/machine-learning-masters-the-fingerprint-to-fool-biometric-systems-300753375.html

Olena, A. (2018). *Bringing the Internet of Things into the Lab*. The Scientist.

Patel, P. (2018). *DNA Data Storage Gets Random Access*. IEEE Spectrum.

Pauwels, E., and Vidyarthi, A. (2017). "Who will own the secrets in our genes? A U.S.-China race in artificial intelligence and genomics," in *Wilson Briefs,* ed W. W. Center (Washington, DC: Woodrow Wilson Center for International Scholars), 5–9.

Podesta, J., Pritzker, P., Moniz, E. J., Holdren, J., and Zientz, J. (2014). *Big Data: Seizing Opportunities, Preserving Values.* ed E.O.O.T. President (Washington, DC).

President's Council of Advisors on Science and Technology (2014). *Big Data and Privacy: A Technological Perspective.* ed E.O.O.T.U.S. President (Washington, DC: White House).

Press, G. (2018). *60 Cybersecurity Predictions for 2019*. Forbes.

Rappeport, A. (2018). *In New Slap at China, U.S. Expands Power to Block Foreign Investments*. The New York Times. Available online at: https://www.nytimes.com/2018/10/10/business/us-china-investment-cfius.html (Accessed November 23, 2018).

Riley, M., and Walcott, J. (2015). *China's Hack of U.S. Data Tied to Health-Care Record Thefts*. Bloomberg UNE.

Roncevich, T. (2018). *Healthcare IT Security Best Practices: Adopting NIST's Cybersecurity Framework. Cyberguard Compliance*. Available online at: https://info.cgcompliance.com/blog/healthcare-it-security-best-practices-adopting-nists-cybersecurity-framework (Accessed Jan 24, 2019).

Sacks, S. (2018). *China's Emerging Data Privacy System and GDPR*. Washington, DC: Center for Strategic and International Studies.

Service, R. F. (2017). DNA could store all of the world's data in one room. *Science*. doi: 10.1126/science.aal0852

Soares, E. (2018). *Brazil: Personal Data Protection Law Enacted. Global Legal Monitor*. Available online at: https://www.loc.gov/law/foreign-news/article/brazil-personal-data-protection-law-enacted/ (Accessed November 23, 2018).

South China Morning Post (2018). *Chinese Funds Pour US$1.4b into US Biotechnology Firms in the First Three Months of the Year*. South China Morning Post. Available online at: https://www.scmp.com/business/global-economy/article/2142351/chinese-funds-pour-us14b-us-biotechnology-firms-first-three (Accessed November 23, 2018).

Souza, C. (2018). *Lessons for Pharma from the Merck Cyber Attack*. PharmExec.com. Available online at: http://www.pharmexec.com/lessons-pharma-merck-cyber-attack (Accessed January 21, 2019).

Thurow, K., Gode, B., Dingerdissen, U., and Stoll, N. (2004). Laboratory information management systems for life science applications. *Org. Proc. Res. Dev.* 8, 970–982. doi: 10.1021/op040017s

Tuzman, K. T. (2018). *Border Security for China's Genomes*. Biocentury Innovations. Available online at: https://www.biocentury.com/bc-innovations/strategy/2018-10-11/balancing-protection-and-translation-china%E2%80%99s-genomic-data-troves

U.S. Congress (2018). *Foreign Investment Risk Review Modernization Act*.

U. S. Government (2012). *United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern*. Washington, DC.

U. S. Government (2014). *United States Government Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern,* Washington, DC.

Von Krogh, G., Battistini, B., Pachidou, F., and Baschera, P. (2012). The changing face of corporate venturing in biotechnology. *Bioentrepreneur* 30, 911–915. doi: 10.1038/bioe.2012.9

Walpole, J., Papin, J. A., and Peirce, S. M. (2013). Multiscale computational models of complex biological systems. *Annu. Rev. Biomed. Eng.* 15, 137–154. doi: 10.1146/annurev-bioeng-071811-150104

Ward, A. (2018). *ISIS's Use of Social Media Still Poses a Threat to Stability in the Middle East and Africa*. RAND. Available online at: https://www.rand.org/blog/2018/12/isiss-use-of-social-media-still-poses-a-threat-to-stability.html (Accessed January 21, 2019).

Wilber, D. Q. (2018). Chinese hackers charged with stealing data from Navy, JPL and U.S. companies. *LA Times*.

You, E. H. (2017). *Safeguarding the Bioeconomy: U.S. Opportunities and Challenges, Testimony for the U.S.-China Economic and Security Review Commission*. Washington, DC: F.B.O. Investigation.

Zhu, J. (2018). *As China Builds Biotech Sector, Cash Floods U.S. Startups*. Reuters. Available online at: https://www.reuters.com/article/us-biotech-china-investment/as-china-builds-biotech-sector-cash-floods-u-s-startups-idUSKCN1M400G (Accessed November 23, 2018).

Disclaimer: The views and conclusions contained herein are those of the authors and should not be interpreted as representing the views and conclusions or official policies and endorsements, either expressed or implied of Griffin Scientific, Promontory Financial Group or the U.S. Government.

Conflict of Interest Statement: KB was employed by Gryphon Scientific. PS was employed by Promontory Financial Group, which is an IBM Company.

The authors declare that the paper was written in the absence of any commercial or financial relationships that would constitute a conflict of interest.

Copyright © 2019 Berger and Schneck. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.