Health Law Institute
2019-10501
Wednesday, March 14, 2019
Session #25: 11:00 a.m. – 12:00 p.m.

Safeguarding the Bioeconomy: Challenges to Data Security, Health and National Security

Edward H. You
Federal Bureau of Investigation
Washington, D.C.

PREPARED STATEMENT OF
EDWARD H. YOU
SUPERVISORY SPECIAL AGENT
BIOLOGICAL COUNTERMEASURES UNIT
COUNTERMEASURES AND OPERATIONS SECTION
WEAPONS OF MASS DESTRUCTION DIRECTORATE
FEDERAL BUREAU OF INVESTIGATION

Safeguarding the Bioeconomy: U.S. Opportunities and Challenges

Testimony for the U.S.-China Economic and Security Review Commission1
March 16, 2017
Prepared Statement Submitted on March 10, 2017

This statement describes the development of the bioeconomy within the United States and China, identifies the opportunities and security challenges facing the United States, and how the United States might better expand the scope of what is determined to be a biological threat and support biotechnology research and industry development for national security.

Background

The Federal Bureau of Investigation (FBI) is the lead law enforcement agency responsible for investigation of Weapons of Mass Destruction (WMD) threats. In particular, the FBI has authorities relating to the investigation, prevention, and response regarding individuals that attempt to obtain or use WMD materials, technology, and expertise. In 2004, the 9/11 Commission recommended that FBI create a new specialized and integrated national security branch to include agents, analysts, linguists, and surveillance specialists to cover the counterterrorism and counterintelligence missions. The WMD Commission Report, generated in response to the anthrax mailings, echoed this recommendation and the FBI responded by creating the National Security Branch (NSB). In 2005, the FBI Director assigned the newly formed NSB to design an operational element to meet the WMD threat. The Weapons of Mass Destruction Directorate (WMD Directorate; WMDD) was created in July 2006, consolidating WMD investigation and prevention efforts to create a unique combination of law enforcement authorities, intelligence analysis capabilities, and technical subject matter expertise focused on chemical, biological, radiological, nuclear, and explosive matters.

Advancements in biotechnologies have led to significant progress such as the production of synthetic microbial genomes and novel methods of pharmaceutical production. The capabilities of these technologies have increased by orders of magnitude over the past few years, and the costs associated with them have decreased by similar orders of magnitude. While these technologies offer amazing promise, they also remain inherently dual-use and just as applicable for nefarious use as reputable use. To that end, the FBI has established various initiatives and working groups, which include the advanced/emerging biotechnology initiative, which is a proactive approach to identify and mitigate current and over-the-horizon risks posed by the exploitation of advancements in research and development of scientific fields such as synthetic biology and genomics. The advanced/emerging biotechnology initiative has FBI partnered with synthetic biology companies to render resources and federal reach-back capabilities to evaluate uncertainties in commercial orders. WMDD is working to develop countermeasures, in

partnership with scientific industry and academia, to prevent adversaries from acquiring and exploiting material and technology that may pose a national security concern. However, biological threat issues have historically focused upon the potential acquisition, development, and use of materials such as viruses, bacteria, and toxins. With the advent of new biotechnologies and the convergence of biology with the cyber/digital realm, current policies and practices to address biological threats may be challenged.

1. **Describe the current status of synthetic biology, genomics, and precision medicine research and applications. What is driving developments in these areas? How, if at all, are artificial intelligence, computing, and data storage playing a role in further advancements? How will advancements in biotechnology affect a country's health, food supply, global competitiveness, and military capabilities?**

Advances in synthetic biology have enabled microbial engineering and facilitated the ability to synthesize and sequence DNA at scale. This has led to the generation of very large data sets and the development of analytical tools as a means to leverage the information for research and practical health applications. The U.S. Precision Medicine Initiative (PMI) is a good example of the direct application of biotechnology and data. PMI is a long-term program that seeks to utilize population genetic data, biological samples, and diet/lifestyle information which are all linked to electronic health records. Research based upon the population data can:

- Advance pharmacogenomics, the right drug for the right patient at the right dose
- Identify new targets for treatment and prevention
- Test whether mobile devices can serve as diagnostic tools and encourage healthy behaviors
- Lay the scientific foundation for precision medicine for many other diseases and conditions

The potential positive impact of PMI to health and the economy has incentivized academia and the private sector to aggregate and agglomerate data from various sources as a means to recapitulate the PMI model. This in turn necessitates the investment and development of artificial intelligence, super-computing, machine learning and algorithm design capabilities as a means to analyze very large data sets and infer causal relationships. The results can then be used to design diagnostics and therapeutics which would benefit existing efforts to bolster national health, biodefense capabilities, and advance countermeasure development. The fundamental aspect of these activities is that the monetization of aggregate data has now transformed it into a significant commodity. However, the challenge is that existing legal frameworks focus upon protecting finished intellectual property or licensed/patented products, whereas large bodies of data, such as patient health records or genetic sequence data, represent near-term, unrealized development of products and applications.

2. **Describe China's access to U.S. genomic data and biological samples. Is this access reciprocal for U.S. researchers and firms? What advantages and disadvantages does this access provide? How is China seeking to expand this access through legal such as joint partnerships or investments and illegal means?**

China has gained significant access to U.S. genomic data and biological samples through research partnerships, investments, mergers, and acquisitions. An example of such access is the accreditation of a China-based DNA sequencing firm by the College of American Pathologists, and as a result, the State of

California is now seeking to export patient samples to the firm for diagnostic processing. Moreover, the storage and transfer of patient health information are strictly regulated within the U.S. (i.e. Health Information Portability and Accountability Act [HIPAA]; Common Rule) preventing sharing of information without consent. Yet, the regulatory frameworks that are put in place to protect patient identity may not apply to the transfer of data overseas. And if breaches or indications of misuse of U.S. person data in an overseas entity are identified, there is no legal recourse for investigation or adjudication by the relevant federal government agencies (Dept. of Health and Human Services and Dept. of Justice).

The current financial environment in the U.S. has also incentivized research institutions and healthcare facilities to contract genetic sequencing services to Chinese or Chinese-affiliated firms. Several major Chinese firms have established genetic sequencing and analytics as a fee-for-service or entered into research collaborations. This has manifested into relationships between U.S. companies, universities, and healthcare facilities. The near term benefits for U.S. entities are realized through acquisition of data to support disease research, health diagnostics, genealogy studies, and personal health information. However, the long-term implications based on China's potential access to the same data (usage contracts notwithstanding) have not been assessed.

Cyber intrusions has had a significant impact on the healthcare sector, affecting millions of U.S. persons. Some of the major intrusions were attributed to China-based hacking groups. The subsequent investigations have focused primarily on the loss of personally identifiable information (PII) or the potential for fraud, as dictated by existing legal frameworks and current threat assessments (HIPAA). However, as described above, data incorporating health conditions, treatments, and diagnoses are qualitatively more valuable than financial/insurance information. Theoretically, the combination of genetic data through research collaborations, legitimate business agreements, and hacked information being exfiltrated to China would be the largest, most diverse dataset ever compiled.

3. Assess the emerging economic and national security risks from the bioeconomy for the United States. How is the U.S. government and industry seeking to address these risks? How successful have those efforts been? What are the remaining challenges? What risks, if any, does China pose to the U.S. bioeconomy?

In 2016 the Obama Administration officially launched PMI with an initial investment of $215 million. By comparison, China announced their own precision medicine initiative with the release of their 13th 5-year plan which will dedicate $9.2 billion USD over a 15-year project. The asymmetry does not exist solely in program funding, but also access to data. As previously described, China may potentially have access to large scale U.S. genomic data through contract work, business partnerships, and research collaborations. However, personal information of Chinese nationals is closely guarded and not shared beyond limited release of very specific data (e.g. biomarkers, database of genomic structural variation [dbGaP]). This was reinforced by the passage of China's Cyber Security Law earlier this year which will provide the government more supervisory jurisdiction over cyberspace, defines security obligations for network operators, and enhances the protection of personal information. In the context of PMI, there is an almost direct correlation between the likelihood of success (i.e. statistical significance) and the size and diversity of the data sets that are analyzed.

Compounding the issues is the fact that biological data is not currently considered "security-related"; therefore, information, such as genetic sequences and electronic health records, is not covered by existing security regimes dealing with export and arms control. As a result, investments, mergers, and acquisitions of U.S. entities may not rise to the level of concern necessitating review and scrutiny for potential security issues (e.g. Committee on Foreign Investments in the U.S. [CFIUS]).

The lack of understanding the breadth and scope of the bioeconomy and the reliance upon the generation and aggregation of data has led to the potential asymmetry in access and capabilities which could impact overall security. If a proper assessment of the vulnerabilities is not conducted to establish the proper balance between protection and innovation, there is a theoretical risk that the U.S. may become marginalized in the global pharmaceutical market and cede the lead in innovation in the burgeoning and dynamic biological-cyber realm. This could have significant implications on the U.S. at the level of the individual, the economy, for biodefense, and overall national security.

4. The Commission is mandated to make policy recommendations to Congress based on its hearings and other research. Assess the implications of China's developments in biotechnology for the United States. What are your specific recommendations for legislative and administrative action?

Since 2014, the FBI WMDD has identified the security issues involving the bioeconomy and has partnered with the American Association for the Advancement of Science (AAAS)[1] and subsequently the National Academies of Sciences (NAS)[2][3]to convene a series of meetings to further elucidate the current and future challenges. Comments regarding the bioeconomy and that were germane to the security issues were provided by meeting participants (these are not formal recommendations or consensus statements):

- Currently, there is no single entity that has the responsibility to assess developments in biotechnology and the impact on the bioeconomy.
- A lack of understanding of the bioeconomy and a focus on biosecurity as it relates to only pathogens and toxins may have left potential gaps in assessing risk and asymmetric access to data.
- The convergence of the life sciences and data science will continue to challenge existing legal frameworks (e.g. HIPAA, export control).
- The holistic assessment of security implications of the bioeconomy must be coupled with activities that will promote U.S. innovation.

[1] https://www.aaas.org/oisa/aaas-fbi/bigdata

[2] https://www.ibpforum.org/resources/safeguarding-bioeconomy-applications-and-implications-emerging-science-meeting-recap

[3] https://www.ibpforum.org/resources/safeguarding-bioeconomy-iii-securing-life-sciences-data-meeting-recap

Links to articles recently released in the news

https://leapsmag.com/bad-actors-getting-your-health-data-is-the-fbis-latest-worry/

https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html