REPORT OF THE UNIFORM LAW COMMISSION
Study Committee on Cybercrime

(ULC Cybercrime Study Committee "Report")

December 15, 2021

Introduction

Cybercrime is a complex term. At high level, it has a plain meaning to the layperson – crimes involving computers. While generally true, this description fails to capture the incredibly complex technological, organizational, cross-jurisdictional, and economic systems within which criminal actors operate. When considering the nature and types of activities the criminal law should punish, this larger context must be considered to ensure both that the criminal law is an adequate deterrence mechanism and that it does not interfere with other important functions of the information economy.

Cybercrime has continuously expanded over the course of the past several decades. Yet most computer crime statutes – "anti-hacking laws" – were enacted before most people even had heard of the Internet, let alone smartphones and wearable technologies. The increase in cybercrime has put pressure on state and local law enforcement resources, which is particularly problematic given the lack of uniformity of cybercrime statutes across U.S. states. In 2019, the National Sheriffs' Association commissioned work urging the Commission to form this Study Committee to examine whether a uniform law should be proposed.

The Commission formed a Study Committee in 2020 to begin addressing these issues and examine whether to proceed with a Drafting Committee. The Study Committee has held several meetings, the product of which highlighted several relevant areas for discussion and to provide further critical background and context regarding the current state of cybercrime issues faced by law enforcement. By the conclusion of these meetings, the Study Committee has agreed to recommend to the Uniform Law Commission (the "Commission") that it constitute a proposed Drafting Committee as outlined below in this Report.

In brief, the Study Committee recommends that the proposed Drafting Committee be charged to consider three areas: (1) substantive criminalization; (2) cybercrime-related criminal procedure; and (3) adjunct and related matters. Section 3 of this Report details those areas. Sections 1 and 2 of this Report provide a summary of the background materials and observations of the Study Committee and a summary of the deliberations of the Study Committee, respectively.

1. Summary of Background Materials Considered and Observations of the Study Committee

The complex and cross-jurisdictional nature in which cybercrime operates poses a significant challenge for efforts to improve enforcement. The Study Committee considered these factors in its deliberations, including specific focus on the complexities of the systems comprising the modern information economy and its inherently cross-jurisdictional nature. This included examining questions related both to the scope of cybercrime and to the governmental and private institutions related to and affected by

cybercrime activities. This Section briefly outlines that scope and gives examples of some related entities and institutions. This is not a comprehensive overview, but rather is designed to help frame an initial discussion in which "cybercrime" is considered as a question beyond mere "unauthorized access" to computing systems.

1.1. Background

Cybercrime has continuously expanded over the course of the past several decades. Yet most computer crime statutes – "anti-hacking laws" – were enacted before most people even had heard of the Internet, let alone smartphones and wearable technologies. The increase in cybercrime has put pressure on state and local law enforcement resources, which is particularly problematic given the lack of uniformity of cybercrime statutes across U.S. states. In 2019, the National Sheriffs' Association commissioned work urging the Commission to form this Study Committee to examine whether a uniform law should be proposed.

The Association summarizes this background well in its March 2019 memorandum:

> Our Subcommittee believes that the cyberthreat will only grow in size and complexity, especially if law enforcement does not become more engaged in combatting the cyberthreat—an outcome we believe unlikely without a comprehensive, forward-looking and uniform set of State cybercrime laws on the States' statutory books.

Other interested constituents have echoed these comments, and they are consistent with the (admittedly limited) scholarly literature and judicial opinions on the subject. The overall backdrop of a "patchwork" of state laws highlights the renewed need for examination of whether – and what – a uniform or model cybercrime statute proposal should cover.

1.2. Examining Questions of Scope

Traditional U.S. cybercrime statutes have focused primarily on "unauthorized access" or "exceeding authorized access" to a computing system, and associated system damage, fraud, and trafficking. In the early 1980s, when 18 U.S.C. § 1030 first was adopted, these did comprise the substantial majority of "computer crimes." In the decades since, however, this landscape has become much more complicated. Computing systems are globally interconnected, consumer and critical infrastructure systems are interconnected, individual identity and financial assets increasingly are more represented and managed by information systems than by tangible documents, and the lines increasingly have blurred between military/national security activities and criminal activities.

For all these reasons, the Study Committee considered a wide variety of potentially-related substantive areas when examining whether (and if so, how) to constitute a Drafting Committee to recommend a uniform cybercrime statute. These factors neither were conceived as exhaustive nor were intended to suggest that all of these categories fall within the scope of a potential uniform cybercrime statute. Indeed, as discussed in Section 3, the Committee concluded that many of the areas considered did *not* fall within the scope of the statutory language. Rather, the Study Committee's work focused on determining what additional areas – both within traditional substantive criminalization and procedure and within related areas – should be considered by a potential future Drafting Committee. The Study Committee should consider the degree to related areas might inform the work of a Drafting Committee, such as by avoiding certain issues or by attempting to account for their overlap.

1.3. Consideration of Related and Affected Institutions and Entities

In addition to the traditional parties the Committee would consult regarding a uniform or model criminal law, the questions of scope addressed in the previous section led the Study Committee to seek input more broadly, including from the following entities:

- American Bar Association
- State/Federal Law Enforcement Officers (current and former)
- Prosecutors (former)
- U.S. Department of Justice
- State Judiciary (former/retired)
- Academics (mostly computer science, public policy, and law)
- Attorneys in Cybercrime-Related Practice
- Consultants and other Cybersecurity Professionals
- Financial Institutions
- Technology Firms
- Cybercrime Public Interest Groups

The Study Committee recognizes that there are other valuable areas from which input could be drawn, but also that there are practical limitations to how much input can be gathered within the duration and scope of its activities. The Committee generally agrees that input from additional sources would not significantly change its recommendations regarding the appointment or scope of a Drafting Committee.

1.4. Background Summary

In summary, the Study Committee examined the question of "cybercrime" broadly, particularly within the context of a cross-disciplinary and cross-jurisdictional[1] nature common to a majority of contemporary cybercrime. The Study Committee began with the default assumption that the States and other U.S. jurisdictions continue to have an important role to play in addressing cybercrime, while remaining open to arguments otherwise. (As noted in Section 3, the Study Committee was unconvinced that cybercrime is purely a Federal issue.) Additionally, the Study Committee recognized that "unauthorized access" and other forms of more "traditional hacking" remain a key focus of substantive cybercrime, and rather looked to this broader examination of "scope" to help the Committee consider a more contemporary perspective of the criminal law's role within a larger cybersecurity ecosystem facing more complex threats from more complex actors.

2. Summary of Committee Discussions

The Study Committee held several meetings over the course of calendar year 2021. A brief summary of those meetings and related drafts and publications is provided below.

[1] Consistent with the Commission's missing, "cross-jurisdictional" refers primarily to the context of acts or organizations crossing state, territorial, or tribal jurisdictions, although international acts and organizations certainly were within the scope of the Study Committee's deliberations to the extent they affected these primary questions.

2.1. Reporter's Introductory Discussion Memorandum – December 23, 2020

Introductory Memorandum Re: ULC Cybercrime Study Committee. Reporter David Thaw prepared an introductory memo dated December 23, 2020, which was distributed to all participants in advance of the first meeting.

2.2. First Meeting – February 8, 2021

At the first virtual meeting, we spent a good deal of time on the introductions of Study Committee members, our Reporter, ABA advisors, and observers, as well as ULC officers and staff. Part of the purpose of this time was to establish a tone of mutual respect for all participants and differing viewpoints. Reporter David Thaw then began a presentation and preliminary discussion of the issues before the committee. We also brainstormed about additional observers.

2.3. Second Meeting – March 22, 2021

The second meeting was a series of presentations by persons connected with the National Sheriff's Association. Sheriff David Goad and Rich Littlehale presented "Benefits for Local Investigation and Prosecutions of a More Uniform State Cybercrime Law Environment". Next, Stacey Wright outlined her work on "The Cyber Classification Compendium". Nick Selby presented "Lessons Learned by NYPD in Operationalizing Public-Facing Cybercrime Investigations". Finally, Dennis Kelly presented "Building a Constituency of Stakeholders Injured by Cybercrime and that would benefit from a 21st Century Uniform Cybercrime Law".

2.4. Third Meeting – May 3, 2021

The third meeting focused on learning about international and national law on cybercrime. First, Betty Shave gave a presentation on the Budapest Convention. She is a former Assistant Deputy Chief at the U.S. Department of Justice and a drafter of the Budapest Convention. Second, Laura-Kate Bernstein, a current Senior Counsel at DOJ, presented on "United States Federal Law on Cybercrime".

2.5. Update re: Observers – May 28, 2021

The Study Committee on Cybercrime had 20 observers as of this date, including from the National Sheriff's Association (that initially proposed this project), federal and state law enforcement agencies, the private sector, and academia. More detail can be found in the report regarding observers. Additional observers were added later as appropriate.

2.6. Reporter's Discussion Memorandum – July 12, 2021

Memorandum Re: ULC Cybercrime Study Committee Discussions ("Reporter's Discussion Memo"). Reporter David Thaw prepared a memo dated July 12, 2021, which proposed a structure for the substantive discussions of the Study Committee on Cybercrime. Specifically, he proposed dividing the discussion into three discrete areas. The first is "substantive criminalization", or what types of acts should primarily be criminalized. The second is "classic criminal procedure matters", covering questions regarding which areas of criminal procedure should be modified or updated to account for a rapidly-changing "cyber" environment. The third is "adjunct and related matters", covering issues such as training and cross-jurisdictional collaboration. This memorandum was distributed to all participants in advance of the July 21, 2021, meeting.

2.7. Fourth Meeting – July 21, 2021

The fourth meeting began with a presentation by Observer Jody Westby, CEO of Global Cyber Risk LLC, together with Mark D. Rasch, of counsel to Korman, Jackson, and Krantz. Following the presentation, Reporter David Thaw began to walk through his July 12, 2021, memo, focusing first on the issue of substantive criminalization. It quickly became clear that there was no consensus yet on the issues of substantive criminalization. Two members of the Study Committee advocated for the position of including no substantive criminal provisions at all in a uniform act. Four members, either at this meeting or through later email correspondence with the Chair Michele Timmons, requested more information but thought that inclusion of a narrowly-tailored group of substantive criminal law provisions might be appropriate.

2.8. Fifth Meeting – September 8, 2021

In advance of this meeting, participants had received a memo dated August 8, 2021, from Observer Dennis Kelly. In addition, a memo dated September 2, 2021, from Observers Jody R. Westby and Gene M. Smith was received and distributed. The Chair spoke first about the divergence of opinions held by members of the Study Committee on the first area of issues surrounding substantive criminal law provisions. She suggested that the group defer further discussion of area #1, and instead move on to areas #2 and #3. Vice Chair Alberto Gonzales led discussion regarding both criminal procedure and adjunct matters. On these two areas, there were substantial areas of consensus.

2.9. Sixth Meeting – October 26, 2021

This meeting was scheduled for a full two hours, to discuss the topic of whether or not substantive criminal provisions should be included in a uniform act. American Bar Association Advisors Jody Westby and Gene Smith, together with Observer Dennis Kelly prepared "Recommendations of the Substantive Provisions Work Group" dated October 21, 2021. In summary, the recommendations sought to include either uniform or model substantive criminal law provisions in an act, essentially following the structure of existing federal law. In support of the recommendations, three brief presentations were made:

- Frank Russo, Director of Government and Legislative Affairs at the National District Attorneys Association (NDAA), stated that harmonized substantive criminal provisions at the state level would improve the ability of district attorneys to prosecute cybercrime.
- Cindy Gonnella, Adjunct Professor, Georgia Institute of Technology, School of Computer Science, also argued for harmonization across state lines, but from the perspective of victims of cybercrime. She gave examples of disappointed cybercrime victims, whose cases were not large enough to warrant federal prosecutions, and were not pursued by local prosecutors because they lacked the harmonized laws, procedures, and knowhow to investigate across state lines.
- John Bandler, founder of Bandler Law Firm PLLC and Bandler Group LLC, and author of 2020 book *Cybercrime Investigations: A Comprehensive Resource for Everyone*, also spoke, emphasizing the need for training and education in order to combat cybercrime.

In addition to these presenters, Stacey Wright gave an update on the Compendium Project. Laws from all fifty states have now been added, and show a substantial difference between the laws in various states. For example, Ms. Wright noted that similar crimes often had different intent standards – one

state might use "knowingly", while another would require "malicious intent". Soon, the Compendium will have a web site link so it is more easily accessible.

Following the presentations, the group discussed the recommendations from the working group. There was favorable discussion regarding the flexibility a potential drafting committee would be given to make substantive criminal provisions *model* or *uniform*. Discussion was more mixed, however, regarding the proposal to model the substantive provisions after federal law; that law has a number of general problems due to its age, and specific problems, such as those raised in the *Van Buren* decision. The ULC Executive Director suggested that the recommendation could be revised to include a minimum list of crimes for a drafting committee to consider.

The Committee and Observers expressed a variety of viewpoints, both in favor and opposing the inclusion of Area 1 issues in a recommendation to the Commission. While consensus regarding a *decision* was not reached at this meeting, the Committee generally agreed that this is a challenging area, and that any consideration of substantive criminalization issues must balance the urgency of cybercrime concerns against the challenges of legislative adoption and overbreadth of the criminal law/unintended consequences of criminalization. The Committee and Observers generally agreed that the U.S. federal Computer Fraud and Abuse Act provided a useful *starting point*, but disagreed as to whether it properly balanced the concerns above. In particular, concerns were expressed both regarding the well-known overbreadth issues of the CFAA, recently limitations in its construction post the Supreme Court's decision in *Van Buren* (as noted above), and other areas that it overlooks (e.g., victim restitution). The Committee and Observers also reiterated the need for education and training, which was discussed as being included in a recommendation for Area 3 (see Section 3.2.3). As noted above, the Committee did generally agree that providing flexibility to a drafting committee to consider both model and uniform legislation would be beneficial.

The Chair stated that another, hopefully final, meeting would be scheduled. The meeting will be to review and discuss a) a revised proposal on substantive provisions, and b) a draft of the Final Report of the Study Committee. That meeting is now scheduled for December 6, 2021.

2.10. Seventh (Final) Meeting – December 6, 2021

The seventh meeting of the Study Committee took place on December 6, 2021 with the primary purpose of reviewing the draft Report for adoption by the Committee.

In advance of this meeting, the Chair distributed the December 3, 2021 draft of this Report as well as a revised memorandum from the Substantive Provisions Work Group (dated November 19, 2021). The Chair spoke first, introducing the topics for discussion and vote which were grouped into the three Area recommendations discussed in Section 3.2.

The Chair first introduced the Substantive Provisions Work Group memo, and then turned the discussion to ABA Advisor Jody Westby to discuss the memo in more detail. Committee members and the Reporter offered comments and observations and the Work Group offered responsive thoughts. Based on this discussion, it was proposed that Section 3.2.1 of this Proposal be edited to include further specific reference to the areas generally criminalized by the CFAA and the Budapest Convention, with inclusion of both the CFAA text and the Work Group's memo as appendices. Additionally, it was proposed that Section 3.2.1 include further specifics regarding the types of Cyber Native crimes that might fall outside

the scope of the CFAA and/or Budapest Convention's existing provisions. The Department of Justice Observer offered one such suggestion (trafficking in botnets).

By polling each individual Study Committee in attendance, the Chair held a vote on the recommendations for Area 1 (substantive criminalization) as discussed in Section 3.2.1 including the revisions above, and the Committee voted to adopt those recommendations, with a request to review the proposed revisions before final sign-off.

The Chair similarly held a vote on the recommendations for Area 2 (criminal procedural) as discussed in Section 3.2.2 and the Committee voted to adopt those recommendations without further modification.

The Chair similarly held a vote on the recommendations for Area 3 (adjunct and related matters) as discussed in Section 3.2.3 and the Committee voted to adopt those recommendations, with one dissent (for concern regarding the fiscal implications) as noted in that Section.

The Chair proposed and the Committee agreed that the Reporter would draft the above-noted revisions for distribution, and that Committee members would send any other proposed line-edits by the end of the day Wednesday, December 8. The meeting adjourned and the Reporter prepared the draft incorporating these revisions and this meeting summary for review by the Chair, Vice-Chair, and ULC Executive Director.

3. Recommendations of the Study Committee

The Study Committee's recommendations are based on the background and discussions summarized above, as well as additional materials presented to the Study Committee. The Study Committee recommends that the Commission form a Drafting Committee, consistent with the specific recommendations outlined below. In summary, these recommendations include:

- Formation of a Drafting Committee to consider uniform and/or model cybercrime legislation at the state/territorial/tribal level
- Encouraging the proposed Drafting Committee to consider Cyber Native and Cyber Enabled[2] crimes as distinguishable categories, with different jurisdictional scope
- Scoping of the proposed Drafting Committee's jurisdiction according to three areas of legislation:
    - Area 1: substantive criminalization of acts/omissions
    - Area 2: frameworks for cybercrime-related criminal procedure
    - Area 3: additional related and/or "adjunct" matters relevant to the investigation or prosecution of cybercrimes

[2] *See* infra Section 3.1 for discussion of the Study Committee's view of Cyber Native and Cyber Enabled crimes.

Furthermore, the Study Committee makes the following recommendations regarding the scope of the proposed Drafting Committee's jurisdiction:

- Regarding Area 1 (substantive criminalization)
  - Full jurisdiction to consider uniform or model legislation for Cyber Native crimes
  - No jurisdiction to consider legislation for Cyber Enabled crimes
  - Limited jurisdiction to consider model legislation for "grey areas" where the proposed Study Committee determines it is unclear whether an act/omission under consideration is Cyber Native or Cyber Enabled
- Regarding Area 2 (criminal procedure)
  - Full jurisdiction to consider uniform or model legislation
  - The Study Committee recommends this as the most important and urgent area of consideration
  - Given this importance and the inherent cross-jurisdictional enforcement issues, the Study Committee strongly encourages the proposed Drafting Committee to pursue uniform legislation for this area
- Regarding Area 3 (related and/or adjunct matters)
  - Full jurisdiction to consider uniform or model legislation
  - The Study Committee notes that most items in this area (e.g., law enforcement training) would likely carry a fiscal note, and encourages the proposed Drafting Committee to be mindful of that limitation when considering uniform vs. model statutory approaches

These recommendations and the bases for them are further detailed in the following subsections.

3.1. Cyber Native and Cyber Enabled Crimes

The Study Committee received presentations and reviewed materials suggesting drawing a distinction between categories of cybercrime activity based on their status as either Cyber Native or Cyber Enabled. Briefly summarized:

- Cyber Native: those crimes which are inherent to, or committed solely/primarily against, an information or computing system (e.g., compromising the security of an electronic commerce system for the purpose of rendering that system inoperable)
- Cyber Enabled: those crimes which already exist as traditional "physical world" crimes but are facilitated by the use of cyber means (e.g., compromising the security of a financial institution's systems for the purpose of misappropriating funds)

The Study Committee views this distinction as important because it is informative regarding approaches a Drafting Committee might adopt when proposing legislation regarding Area 1 (substantive criminalization).[3] In particular, the Study Committee recommends the proposed Drafting Committee review the materials received by the Study Committee in this regard and further engage substantive

[3] It may also be generally informative for Areas 2 (criminal procedure) and 3 (adjunct and related matters) to the extent there are specific instances where the distinction matters, however the Study Committee does not recommend its use as a tool for primary distinction regarding issues in Areas 2 and 3.

experts (whether as Observers or presenters) in a position to comment on the nature of various approaches to statutory drafting.

This engagement of additional substantive experts is particularly important in the context of Area 1, especially given the decades-long struggles regarding the ambiguities of the federal cybercrime legislation captured in the Computer Fraud and Abuse Act of 1986 (codified as amended at 18 U.S.C. § 1030), ambiguities within which remain the subject of ongoing appellate review as recently as the October Term 2020 of the U.S. Supreme Court (*see Van Buren v. United States*, No. 19-783 (2021) (holding in relevant part that unauthorized access or exceeding authorized access does not extend do "improper motives" for accessing information which an employee-user of a state government agency has technological access, but to which policies would otherwise permit such access based on "improper motive"). The result of this struggle is a tension between a desire to ensure the scope of the criminal law adequately covers serious cybercrimes, while at the same time not creating a circumstance where non-technical users of computing systems are unable to discern what they are or are not permitted to do in advance.

This well-known debate regarding the Computer Fraud and Abuse Act of 1986 (CFAA) is an ambiguity which has challenged access-based statutory language for decades, in large part because of its nature tending to make such statutory language both overbroad and underinclusive. For example, it is a well-established principle in U.S. law that private parties should not be able to define the scope and application of the criminal law through private contracts of which a criminal defendant may have little or no effective notice.[4] Yet it is also a well-established principle that the owners of private property should be able to grant access solely for specific purposes, without waiving their right to protection by trespass, burglary, or other similar property-breach laws by a person accessing property outside those purposes.[5] The "access without authorization" principle opens the door to both possibilities, and has been widely criticized on both points. In short, while a useful principle within the context of theoretical cybersecurity, its reductionist nature is difficult to translate to the more context-specific and highly nuanced area of the criminal law.

The Cyber Native vs Cyber Enabled distinction is by no means a panacea to addressing these defects. However, the Study Committee recommends that the proposed Drafting Committee can make progress by adopting this distinction, and focusing its work on developing language that expands the scope to address potential "gaps" in the access-without-authorization regime, while at the same time not sweeping so broadly as to criminalize anonymous speech, misrepresenting one's physical appearance on a dating website, or similarly engaging in violations of terms-of-service that most cybersecurity experts would not traditionally view as "hacking" or "cracking" a system.[6]

---

[4] *See, e.g., United States v. Drew*, 259 F.R.D. 449 (C.D. Cal 2009).

[5] Consider, for example, the implied right of access to approach a house granted to a sidewalk, but not extending further to other parts of the property or other procedures in the implied area inside the curtilage. *See, e.g., Florida v. Jardines*, 569 U.S. 1104 (2013) (holding in relevant part that a police search by a trained, drug-sniffing dog, conducted while approaching the home via the front walkway, extended beyond the implied license of an average person to walk up to the door, knock, wait briefly, and then leave (if not invited to remain)).

[6] *See, e.g., United States v. Drew*, supra n. 4, *see also e.g., United States v. Auernheimer*, 748 F.3d 525 (3d Cir. 2014) (dismissing and vacating the conviction for lack of venue, but also noting the "number of complex and novel issues

This is, of course, not to say that Cyber Enabled crimes are not more severe than their physical world counterparts, nor that Cyber Enabled crimes should not be considered within the jurisdiction of the proposed Drafting Committee. The purpose of this distinction is only to highlight differences for consideration against a backdrop of problems created by attempting to translate (appropriately) reductionist theoretical scientific principles[7] to a legal framework without proper contextualization.

Finally, it is important to recognize that Cyber Native and Cyber Enabled will not always constitute a bright-line distinction. There are likely to be many "grey areas" or edge cases, and the Study Committee encourages the proposed Drafting Committee to be mindful of these circumstances where the two may overlap, blend together, or otherwise be difficult clearly to delineate.

In summary, the Study Committee recommends that considering a distinction between Cyber Native and Cyber Enabled crimes will facilitate the work of the proposed Drafting Committee and assist their engagement of experts in the drafting of proposed statutory language.

3.2. Areas for Consideration by the Proposed Drafting Committee

The Study Committee recommends that the proposed Drafting Committee organize its work into three primary areas. These areas are not necessarily exclusive, but rather highlight the major areas examined in the Study Committee's discussions and the proposal the Study Committee believes will best balance the various goals and challenges examined in the Study Committee's research and deliberations.

3.2.1. Area 1: Substantive Criminalization

The question of substantive criminalization is the class ambit of the criminal law – to prohibit certain acts or omissions by utilizing the power of the government to physically punish those who fail to comply with such prohibitions. It is a power to be exercised judiciously and with care. While there was some debate within the Study Committee as to the full scope to which a Drafting Committee should consider such matters, the evidence presented to the Study Committee and its deliberations generally converged on a need to recommend that the proposed Drafting Committee examine this area as follows and for the reasons explained therein.

The cross-jurisdictional nature of cybercrime creates challenges when jurisdictions have different substantive criminal prohibitions – even if those prohibitions were intended by the respective legislatures generally to prohibit the same types of acts. This is particularly true given the rise of Cyber Native crimes discussed in Section 3.1 above. Furthermore, both Federal legislation and most U.S. states' cybercrime statutes are decades old – an eternity in "Internet" time – and leave gaps both

---

that are of great public importance in our increasingly interconnected age" raised by the parties on appeal, and discussing the facts behind such issues in Part I(A) of the Opinion).

[7] In relevant part, the commonly cited "CIA framework" – confidentiality, integrity, and availability – of cybersecurity is often referenced as a basis for access-without-authorization frameworks of computer crime statutes. The CIA framework is an excellent computer science teaching tool, and also an excellent tool for formal proof. It is less useful, however, in practical interdisciplinary application, primarily because of this reductionist nature. *See* Derek E. Bambauer, Justin (Gus) Hurwitz, David Thaw, and Charlotte A. Taschider, CYBERSECURITY: AN INTERDISCIPLINARY PROBLEM at 29-35 (2021) (discussing the CIA model and its limits as a function of being reductionist, particularly in the context of practical application as opposed to computer science theory).

resulting from antiquated frameworks[8] and the translation of theoretical computer science to practical application without contextualization.[9] As a result, it is the observation of the Study Committee that current cybercrime laws have the potential both to be underinclusive and overbroad – failing to prohibit those acts which cause significant harm to society, while concurrently providing the opportunity for non-judicious use of the criminal law to punish acts not necessarily contemplated by the legislatures.

As discussed above, the Study Committee recommends that considering a distinction between Cyber Native and Cyber Enabled crimes can help address these concerns. First, it draws attention to those categories of acts or omissions which may have arisen in recent years and been outside the consideration of the legislatures (indeed, not yet invented) when cybercrime statutes first were adopted. Second, it cabins off the question of increased penalties for extant prohibited acts/omissions when committed using cyber means – a separate, potentially important question on which the Study Committee did not significantly focus – thus reducing the risk of "unintended consequences" affecting areas outside the scope of the Study Committee's consideration and more likely to be perceived by differently legislatures as a policymaking matter.[10]

Considering all these factors, those presented in earlier sections of this Report, and the Study Committee's deliberations, the Study Committee recommends to the Commission that the proposed Drafting Committee be granted the jurisdiction to consider legislation with the area of substantive criminalization. More specifically, and in line with these discussions the Study Committee recommends that the proposed Drafting Committee have jurisdiction to consider model or uniform legislation regarding Cyber Native crimes.

The Study Committee recommends that the proposed Drafting Committee not be charged with directly considering Cyber Enabled crimes. However, the Study Committee recognizes the potential for overlap and "grey areas," and accordingly recommends that within the context of areas the proposed Drafting Committee is unable clearly to classify as Cyber Native or Cyber Enabled, or where clear overlap exists, they be granted jurisdiction to consider only bracketed or optional legislative text for these areas. Furthermore, the Study Committee notes that many of the concerns raised in its deliberations in the presentations it received regarding Cyber Enabled crimes may be addressed by some of the work the proposed Drafting Committee might undertake for Area 2 (cybercrime-related criminal procedure).

The Study Committee did not undertake comprehensive examination and deliberations regarding precisely what should be the content of any updates beyond the recommendations above, opting instead to leave those questions to the proposed Drafting Committee. However, the Study Committee notes for the benefit of the Commission and of the proposed Drafting Committee, that both the federal Computer Fraud and Abuse Act ("CFAA") and the Budapest Convention on Cybercrime provide starting

[8] For example, the Internet and the World Wide Web, as construed in their modern form, was not commercially available to the public at the time the Computer Fraud and Abuse Act was first passed by the U.S. Congress.
[9] See further discussion of this issue in Section 3.1 supra.
[10] For example, consider the case of "cyberbullying" – a classic Cyber Enabled crime. Some legislatures may wish to have increased penalties for this type of activity as compared to traditional non-battery assault, whereas other legislatures may not (or may elect not to criminalize non-battery assault at all). While such considerations may be the proper province of *a different* ULC Study Committee, making a comprehensive recommendation on cyberbully was far outside the scope of this Study Committee's charge.

points for consideration, in particular the types of Cyber Native crimes which new technologies may have enabled since the original drafting of the CFAA and the Budapest Convention.

The Study Committee further notes the potential for underinclusiveness and overbreadth in both and encourages the proposed Drafting Committee to view its work as an opportunity to make progress addressing these important and significant debates.

For example, the Study Committee recommends that the proposed Drafting Committee consider the core concepts of access, authorization, damage, and computer-specific fraud (e.g., from the CFAA)[11] and the core concepts of illegal access, illegal interception, data interference, system interference, device misuse, computer-related forgery, computer-related fraud (e.g., from Titles 1, 2 and 5 of the Budapest Convention).[12] The concepts of inchoate and accomplice liability should also be considered by a proposed Drafting Committee as they appear both in the CFAA and Budapest Convention, as well as many (if not most) of the extant state statutes covering computer crimes. The Study Committee also recommends further that the proposed Drafting Committee consider any additional Cyber Native crimes which may not be strictly swept within these frameworks in addressing the potential underinclusiveness problem.

3.2.2.Area 2: Cybercrime-related Criminal Procedure

The Study Committee is in strong agreement that the most important area for consideration by the proposed Drafting Committee is legislation regarding cybercrime-related criminal procedure. Cross-jurisdictional collaboration around many aspects of the investigative and prosecutorial processes were viewed by members of and presenters to the Committee as one of the most apparent "weak links" in the cybercrime enforcement ecosystem. In this regard, the Study Committee recommends that the proposed Drafting Committee have full jurisdiction to consider any relevant model or uniform legislation. Furthermore, the Study Committee recommends that uniform legislation, at least as to the investigative and evidentiary procedures, would have significant benefit for law enforcement. Accordingly, if the proposed Drafting Committee adopts model legislation, the Study Committee encourages them to strongly convey the limitations of current cross-jurisdictional frameworks.

It is not the recommendation of the Study Committee to limit the scope of this area (either in the context of investigative vs. adjudicative procedure, or in the context of Cyber Native vs. Cyber Enabled Crimes), and recommends the Commission broadly construe its charge to the proposed Drafting Committee, subject to two caveats. First, the primary focus of the concerns motivating the Study Committee's recommendations are inability adequately to enforce cybercrime laws as a result of procedural inconsistencies or incompatibilities. The Study Committee did not undertake, and does not opine on, the need for criminal procedure reform writ large. Rather it urges the proposed Drafting Committee to review the materials considered by the Study Committee and to engage expertise focused on this enforcement question.

Second, the Study Commission issues a standard caution regarding any procedural matters which may inherently or optionally result in fiscal implications. While the Study Committee does not discourage the

[11] *See* Appendix A, Computer Fraud and Abuse Act of 1986 (codified as amended at 18 U.S.C. § 1030).
[12] *See* Appendix B, Jody R. Westby, Gene M. Smith, Dennis Kelly & Betty Shave, *Revised Recommendation of the Substantive Provisions Work Group* (Nov. 19, 2021).

proposed Drafting Committee from recommending such reforms, it does encourage the proposed Drafting Committee to consider reframing such proposals within the context of Area 3, for the purposes of separating out those items most likely to carry a fiscal note and improving the probability of achieving the primary goal – procedural standardization or at least moderate harmonization (for compatibility) in cybercrime enforcement across U.S. jurisdictions.

To facilitate the primary goal of improving cross-jurisdictional cybercrime enforcement, the Study Committee recommends that the proposed Drafting Committee examine the full scope criminal procedure legislation from investigative to adjudicative procedures. While the Study Committee highlights several examples in the following paragraphs including specific recommendations for areas of high importance within the investigative areas of criminal procedure, the Study Committee recognizes that it had exceptional expertise in this area and encourages the proposed Drafting Committee to engage similar relevant expertise in the adjudicative areas of criminal procedure (e.g., from state cybercrime prosecutors or state criminal courts) as well to examine what possible proposed legislation in that area could facilitate cross-jurisdictional enforcement as well.

First, regarding investigative criminal procedure, the Study Committee recommends that the proposed Drafting Committee evaluate issues relating to electronic searches, evidence authentication, and evidence laboratory standards, administration, and cyber-related operations and policy. The Study Committee had a strong consensus that these examples and related topics are of paramount importance to addressing issues related to cross-jurisdictional enforcement and related issues currently challenging cybercrime enforcement.

Second, regarding investigative criminal procedure, the Study Committee recommends that the proposed Drafting Committee evaluate issues regarding searches, seizures, and other compelled production of evidence. The Study Committee had strong consensus regarding these examples as well. Furthermore, the Study Committee recommends the proposed Drafting Committee consider issues related to compelled disablement of electronic systems other than by seizure (sometimes referred to as "takedown" procedures), but felt more information was needed to determine the extent to which this is properly within the scope of criminal (as opposed to civil or regulatory) law.

Third, regarding the concept of multi-state compacts, the Study Committee generally agreed that the proposed Drafting Committee should examine them, but cautions that such compacts generally operate contrary to the idea of a "uniform" statute and the proposed Drafting Committee may want to limit its examination to any bracketed or optional language which could enable such compacts (e.g., on an *ad hoc* basis) in jurisdictions where the lack of such enabling language could hamper cross-jurisdictional collaboration on specific matters.[13]

Fourth, as noted above, the Study Committee generally recommends that the proposed Drafting Committee neither limit itself to either of Cyber Enabled or Cyber Native crimes, nor limit itself only to either of investigative or adjudicative criminal procedure, but rather consider all relevant areas of criminal procedure as within its potential scope for proposing legislative language.

[13] E.g., if a jurisdiction – for lack of general enabling language – required legislative approval for each such multi-jurisdictional investigative operation, where such legislative process would be sufficiently time-consuming as to offset any benefits realized from the collaboration itself.

Fifth, the Study Committee generally agreed that issues surrounding evidence preservation generally were of significant import, but recognizes that (similar to the question of "takedowns") these may overlap with civil or regulatory processes, and recommends the proposed Drafting Committee be mindful of such potential overlap to the extent it elects to make recommendations in this regard beyond the traditional scope of investigative and adjudicative criminal procedure.

Finally, the Study Committee wishes again to reiterate the importance of this area to facilitating progress on cross-jurisdictional cybercrime enforcement. There was general agreement that this area is the most important among the topics discussed, has the most potential to make the greatest impact, and would most benefit from state-level uniformity. Furthermore, the Study Committee believes this is the most urgent among its recommendations as existing incompatibilities and inconsistencies in procedure across states, territories, and tribal nations has the greatest impact on impeding cross-jurisdictional cybercrime enforcement.

3.2.3. Area 3: Adjunct and Related Matters

Many of the issues discussed regarding enforcement inevitably raised questions of matters related to procedure or substantive criminalization, but which generally are not considered directly to be a part of those areas in a formal legal definition. This area covers those aspects of legislation and administrative recommendations which relate to, but are not formally part of, the two categories above. Many topics within this area may be as critical as those above, and should not be viewed as inferior or subordinate. Rather, it is important to separate these from the two areas above as they involve different fundamental questions, and because they often involve different areas of law (e.g., administrative law, state/local government law, appropriations and fiscal policy).

While this category is not intended to be a "catch-all," the Study Committee is mindful that it may have this effect – partially as a function of the doctrinal division sometimes found in criminal law into "substantive prohibitions," "procedure," and "everything else." The Study Committee encourages the proposed Drafting Committee not to consider it as such, but rather to consider it as a third category for important and clearly related matters not properly fitting into Areas 1 or 2, or otherwise properly delineated from items in those Areas (e.g., for fiscal reasons), as discussed above and further in this Section.

The most common example considered by the Study Committee was that of investigative and prosecutorial training. Cybercrime is an inherently technical subject-matter area, but unlike other such areas (e.g., financial crimes), cybercrime is pervasive across many other areas of criminal law enforcement. This is particularly true because of the increasing prevalence of traditional physical-world crimes committed through or enhanced by cyber means (Cyber Enabled crimes). This area appears to be of significant importance to many state and local law enforcement officials, and the Study Committee believes that even just the inclusion of optional or bracketed language, notwithstanding the necessary fiscal implications, could have the potential to motivate further recognition of the importance of these issues by policymakers.

The Study Committee also recommends that the proposed Drafting Committee be charged with examining legislative language to facilitate evidentiary data, investigative and adjudicative metadata (e.g., criminal activity report frequency), and other relevant information across jurisdictions. The Study Committee notes, however, that any such legislative language should carefully consider appropriate

confidentiality restrictions regarding any relevant superseding Constitutional or federal privacy law issues, as well as federal and state constitutional protections for criminal investigations. Information sharing activities of this type will most effectively benefit cybercrime enforcement if such legislation facilitates resolution of these related policy issues, rather than further exacerbating or complicating their debate.[14]

The Study Committee does not have a recommendation for solving the inherent likelihood of fiscal implications attached to these items, but recommends that the proposed Drafting Committee consider using bracketed or optional provisions for items necessarily carrying fiscal notes. The Study Committee does recommend acknowledging the inherent or probable need for fiscal notes when applicable, and recommends the proposed Drafting Committee take such matters into account when considering which aspects of this area should be proposed as uniform legislation or proposed as model legislation. Nonetheless, the Study Committee does recommend that the Commission constitute the proposed Drafting Committee with full authority to consider all approaches for this Area.

The Committee notes for the record that there was one dissenting vote regarding the recommendations for this Area, the basis for which was concern regarding the fiscal implications of the recommendations contained herein.

4. Conclusions

In conclusion, the Study Committee recommends that the Commission constitute a Drafting Committee on cybercrime legislation according to the specific recommendations above. The Study Committee recommends that the work of the proposed Drafting Committee be organized, and urges the proposed Drafting Committee to consider its work within the complex ecosystem of cybercrime summarized throughout this Report and discussed further in the materials provided by the Study Committee.

Respectfully,

Uniform Law Commission Study Committee on Cybercrime

Michele Timmons, Chair

Alberto R. Gonzales, Vice-Chair

David Thaw, Reporter

[14] For example, a cross-jurisdictional information sharing regime, the result of which results in evidence suppression on federal Constitutional grounds, would not advance the state of cybercrime enforcement. By contrast, one designed with these issues in mind specifically, and that creates an effective "safe harbor" by which such sharing can occur with limited risk of evidentiary suppression or exclusion, would likely significantly improve enforcement efforts and collaboration incentives.

Appendix A

The Computer Fraud and Abuse Act of 1986

18 U.S.C. § 1030

(retrieved from the Government Printing Office official website, December 14, 2021)

https://www.govinfo.gov/content/pkg/USCODE-2010-title18/pdf/USCODE-2010-title18-partI-chap47-sec1030.pdf

Subsec. (a)(6). Pub. L. 103–414, § 206(a)(2), added par. (6) relating to scanning receivers or other hardware or software used to obtain unauthorized access to telecommunications services.

Pub. L. 103–322, § 250007(1)(B), added par. (6) relating to solicitations which offer access devices or information regarding access devices.

Subsec. (a)(7). Pub. L. 103–322, § 250007(1)(B), added par. (7).

Subsec. (c)(1). Pub. L. 103–322, § 330016(2)(I), substituted ''fine under this title or twice the value obtained by the offense, whichever is greater, or imprisonment'' for ''fine of not more than the greater of $10,000 or twice the value obtained by the offense or imprisonment''.

Pub. L. 103–322, § 250007(2), substituted ''(a)(2), (3), (5), (6), or (7)'' for ''(a)(2) or (a)(3)''.

Subsec. (c)(2). Pub. L. 103–414, § 206(b), substituted ''(a)(1), (4), (5), or (6)'' for ''(a)(1) or (a)(4)''.

Pub. L. 103–322, § 330016(2)(I), substituted ''fine under this title or twice the value obtained by the offense, whichever is greater, or imprisonment'' for ''fine of not more than the greater of $50,000 or twice the value obtained by the offense or imprisonment''.

Subsec. (c)(3). Pub. L. 103–322, § 330016(2)(I), substituted ''fine under this title or twice the value obtained by the offense, whichever is greater, or imprisonment'' for ''fine of not more than the greater of $100,000 or twice the value obtained by the offense or imprisonment''.

Subsec. (e)(1). Pub. L. 103–414, § 206(c)(1), inserted ''electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier,'' after ''account number,''.

Subsec. (e)(5), (6). Pub. L. 103–322, § 250007(3)(A), (B), and Pub. L. 103–414, § 206(c)(2), (3), amended subsec. (e) identically, striking ''and'' at end of par. (5) and substituting ''; and'' for period at end of par. (6).

Subsec. (e)(7). Pub. L. 103–414, § 206(c)(4), added par. (7) defining ''scanning receiver''.

Pub. L. 103–322, § 250007(3)(C), added par. (7) defining ''credit card system member''.

1990—Subsec. (f). Pub. L. 101–647 inserted at end ''For purposes of this subsection, the term 'State' includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.''

1986—Subsec. (f). Pub. L. 99–646 which directed that subsec. (f) be amended by substituting ''chapter 224 of this title'' for ''title V of the Organized Crime Control Act of 1970 (18 U.S.C. note prec. 3481)'' was executed by making the substitution for ''title V of the Organized Crime Control Act of 1970) 18 U.S.C. note prec. 3481)'' to reflect the probable intent of Congress.

TRANSFER OF FUNCTIONS

For transfer of the functions, personnel, assets, and obligations of the United States Secret Service, including the functions of the Secretary of the Treasury relating thereto, to the Secretary of Homeland Security, and for treatment of related references, see sections 381, 551(d), 552(d), and 557 of Title 6, Domestic Security, and the Department of Homeland Security Reorganization Plan of November 25, 2002, as modified, set out as a note under section 542 of Title 6.

REPORT TO CONGRESS

Section 1603 of Pub. L. 98–473 directed Attorney General to report to Congress annually, during first three years following Oct. 12, 1984, concerning prosecutions under this section.

§ 1030. Fraud and related activity in connection with computers

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.[1]

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

[1] So in original. The period probably should be a semicolon.

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;[2]

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4),[3] or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(4)(A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of—

(i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)—

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV) a threat to public health or safety;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

(VI) damage affecting 10 or more protected computers during any 1-year period; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i) an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or

(ii) an attempt to commit an offense punishable under this subparagraph;

(C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of—

(i) an offense or an attempt to commit an offense under subparagraphs (A) or (B) of

[2] So in original. Probably should be followed by ''or''.

[3] So in original. The comma probably should not appear.

subsection (a)(5) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i) an offense or an attempt to commit an offense under subsection (a)(5)(C) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;

(F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or

(G) a fine under this title, imprisonment for not more than 1 year, or both, for—

(i) any other offense under subsection (a)(5); or

(ii) an attempt to commit an offense punishable under this subparagraph.

(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section—

(1) the term ''computer'' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term ''protected computer'' means a computer—

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3) the term ''State'' includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term ''financial institution'' means—

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a)[4] of the Federal Reserve Act;

(5) the term ''financial record'' means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term ''exceeds authorized access'' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7) the term ''department of the United States'' means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8) the term ''damage'' means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term ''government entity'' includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10) the term ''conviction'' shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term ''loss'' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage

[4] See References in Text note below.

assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term ''person'' means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses[5] (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

(i)(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

(A) such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

(B) any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:

(1) Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(2) Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section[6]

(Added Pub. L. 98–473, title II, § 2102(a), Oct. 12, 1984, 98 Stat. 2190; amended Pub. L. 99–474, § 2, Oct. 16, 1986, 100 Stat. 1213; Pub. L. 100–690, title VII, § 7065, Nov. 18, 1988, 102 Stat. 4404; Pub. L. 101–73, title IX, § 962(a)(5), Aug. 9, 1989, 103 Stat. 502; Pub. L. 101–647, title XII, § 1205(e), title XXV, § 2597(j), title XXXV, § 3533, Nov. 29, 1990, 104 Stat. 4831, 4910, 4925; Pub. L. 103–322, title XXIX, § 290001(b)–(f), Sept. 13, 1994, 108 Stat. 2097–2099; Pub. L. 104–294, title II, § 201, title VI, § 604(b)(36), Oct. 11, 1996, 110 Stat. 3491, 3508; Pub. L. 107–56, title V, § 506(a), title VIII, § 814(a)–(e), Oct. 26, 2001, 115 Stat. 366, 382–384; Pub. L. 107–273, div. B, title IV, §§ 4002(b)(1), (12), 4005(a)(3), (d)(3), Nov. 2, 2002, 116 Stat. 1807, 1808, 1812, 1813; Pub. L. 107–296, title II, § 225(g), Nov. 25, 2002, 116 Stat. 2158; Pub. L. 110–326, title II, §§ 203, 204(a), 205–208, Sept. 26, 2008, 122 Stat. 3561, 3563.)

REFERENCES IN TEXT

Section 11 of the Atomic Energy Act of 1954, referred to in subsec. (a)(1), is classified to section 2014 of Title 42, The Public Health and Welfare.

The Fair Credit Reporting Act, referred to in subsec. (a)(2)(A), is title VI of Pub. L. 90–321, as added by Pub. L. 91–508, title VI, § 601, Oct. 26, 1970, 84 Stat. 1127, as amended, which is classified generally to subchapter III (§ 1681 et seq.) of chapter 41 of Title 15, Commerce and Trade. For complete classification of this Act to the Code, see Short Title note set out under section 1601 of Title 15 and Tables.

The Farm Credit Act of 1971, referred to in subsec. (e)(4)(E), is Pub. L. 92–181, Dec. 10, 1971, 85 Stat. 583, as amended, which is classified generally to chapter 23 (§ 2001 et seq.) of Title 12, Banks and Banking. For complete classification of this Act to the Code, see Short Title note set out under section 2001 of Title 12 and Tables.

Section 15 of the Securities Exchange Act of 1934, referred to in subsec. (e)(4)(F), is classified to section 78*o* of Title 15, Commerce and Trade.

Section 1(b) of the International Banking Act of 1978, referred to in subsec. (e)(4)(H), is classified to section 3101 of Title 12, Banks and Banking.

Section 25 of the Federal Reserve Act, referred to in subsec. (e)(4)(I), is classified to subchapter I (§ 601 et seq.) of chapter 6 of Title 12. Section 25(a) of the Federal Reserve Act, which is classified to subchapter II (§ 611 et seq.) of chapter 6 of Title 12, was renumbered section 25A of that act by Pub. L. 102–242, title I, § 142(e)(2), Dec. 19, 1991, 105 Stat. 2281.

The date of the enactment of this subsection, referred to in subsec. (h), is the date of enactment of Pub. L. 103–322, which was approved Sept. 13, 1994.

AMENDMENTS

2008—Subsec. (a)(2)(C). Pub. L. 110–326, § 203, struck out ''if the conduct involved an interstate or foreign communication'' after ''computer''.

Subsec. (a)(5). Pub. L. 110–326, § 204(a)(1), redesignated cls. (i) to (iii) of subpar. (A) as subpars. (A) to (C), respectively, substituted ''damage and loss.'' for ''damage; and'' in subpar. (C), and struck out former subpar. (B) which read as follows:

''(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United

[5] So in original. Probably should be ''subclause''.

[6] So in original. Probably should be followed by a period.

States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety; or

''(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;''.

Subsec. (a)(7). Pub. L. 110–326, §205, amended par. (7) generally. Prior to amendment, par. (7) read as follows: ''with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;''.

Subsec. (b). Pub. L. 110–326, §206, inserted ''conspires to commit or'' after ''Whoever''.

Subsec. (c)(2)(A). Pub. L. 110–326, §204(a)(2)(A), struck out ''(a)(5)(A)(iii),'' after ''(a)(3),''.

Subsec. (c)(3)(B). Pub. L. 110–326, §204(a)(2)(B), struck out ''(a)(5)(A)(iii),'' after ''(a)(4),''.

Subsec. (c)(4). Pub. L. 110–326, §204(a)(2)(C), amended par. (4) generally. Prior to amendment, par. (4) related to fines and imprisonment for intentionally or recklessly causing damage to a protected computer without authorization.

Subsec. (c)(5). Pub. L. 110–326, §204(a)(2)(D), struck out par. (5) which related to fine or imprisonment for knowingly or recklessly causing or attempting to cause serious bodily injury or death from certain conduct damaging a protected computer.

Subsec. (e)(2)(B). Pub. L. 110–326, §207, inserted ''or affecting'' after ''which is used in''.

Subsec. (g). Pub. L. 110–326, §204(a)(3)(B), in the third sentence, substituted ''subsection (c)(4)(A)(i)(I)'' for ''subsection (a)(5)(B)(i)''.

Pub. L. 110–326, §204(a)(3)(A), which directed substitution of ''in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)'' for ''in clauses (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B)'' in the second sentence, was executed by making the substitution for ''in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B)'' to reflect the probable intent of Congress.

Subsecs. (i), (j). Pub. L. 110–326, §208, added subsecs. (i) and (j).

2002—Subsec. (a)(5)(B). Pub. L. 107–273, §4005(a)(3), realigned margins.

Subsec. (c)(2)(B). Pub. L. 107–273, §4002(b)(1), realigned margins.

Subsec. (c)(2)(B)(iii). Pub. L. 107–273, §4002(b)(12)(A), inserted ''and'' at end.

Subsec. (c)(3)(B). Pub. L. 107–273, §4005(d)(3), inserted comma after ''(a)(4)''.

Subsec. (c)(4)(A), (C). Pub. L. 107–296, §225(g)(2), inserted ''except as provided in paragraph (5),'' before ''a fine under this title''.

Subsec. (c)(5). Pub. L. 107–296, §225(g)(1), (3), (4), added par. (5).

Subsec. (e)(4)(I). Pub. L. 107–273, §4002(b)(12)(B), substituted semicolon for period at end.

2001—Subsec. (a)(5)(A). Pub. L. 107–56, §814(a)(1)–(3), designated existing provisions as cl. (i), redesignated subpars. (B) and (C) as cls. (ii) and (iii), respectively, of subpar. (A), and inserted ''and'' at end of cl. (iii).

Subsec. (a)(5)(B). Pub. L. 107–56, §814(a)(4), added subpar. (B). Former subpar. (B) redesignated cl. (ii) of subpar. (A).

Subsec. (a)(5)(C). Pub. L. 107–56, §814(a)(2), redesignated subpar. (C) as cl. (iii) of subpar. (A).

Subsec. (a)(7). Pub. L. 107–56, §814(b), struck out '', firm, association, educational institution, financial institution, government entity, or other legal entity,'' before ''any money or other thing of value''.

Subsec. (c)(2)(A). Pub. L. 107–56, §814(c)(1)(A), inserted ''except as provided in subparagraph (B),'' before ''a fine'', substituted ''(a)(5)(A)(iii)'' for ''(a)(5)(C)'', and struck out ''and'' at end.

Subsec. (c)(2)(B). Pub. L. 107–56, §814(c)(1)(B), inserted ''or an attempt to commit an offense punishable under this subparagraph,'' after ''subsection (a)(2),'' in introductory provisions.

Subsec. (c)(2)(C). Pub. L. 107–56, §814(c)(1)(C), struck out ''and'' at end.

Subsec. (c)(3). Pub. L. 107–56, §814(c)(2), struck out '', (a)(5)(A), (a)(5)(B),'' after ''subsection (a)(4)'' in subpars. (A) and (B) and substituted ''(a)(5)(A)(iii)'' for ''(a)(5)(C)'' in subpar. (B).

Subsec. (c)(4). Pub. L. 107–56, §814(c)(3), added par. (4).

Subsec. (d). Pub. L. 107–56, §506(a), amended subsec. (d) generally. Prior to amendment, subsec. (d) read as follows: ''The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.''

Subsec. (e)(2)(B). Pub. L. 107–56, §814(d)(1), inserted '', including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States'' before semicolon.

Subsec. (e)(7). Pub. L. 107–56, §814(d)(2), struck out ''and'' at end.

Subsec. (e)(8). Pub. L. 107–56, §814(d)(3), added par. (8) and struck out former par. (8) which read as follows: ''the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information, that—

''(A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals;

''(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

''(C) causes physical injury to any person; or

''(D) threatens public health or safety; and''.

Subsec. (e)(10) to (12). Pub. L. 107–56, §814(d)(4), (5), added pars. (10) to (12).

Subsec. (g). Pub. L. 107–56, §814(e), substituted ''A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages.'' for ''Damages for violations involving damage as defined in subsection (e)(8)(A) are limited to economic damages.'' and inserted at end ''No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.''

1996—Subsec. (a)(1). Pub. L. 104–294, §201(1)(A), substituted ''having knowingly accessed'' for ''knowingly accesses'', ''exceeding authorized access'' for ''exceeds authorized access'', ''such conduct having obtained information'' for ''such conduct obtains information'', and ''could be used to the injury of the United States'' for ''is to be used to the injury of the United States'', struck out ''the intent or'' before ''reason to believe'', and inserted before semicolon at end ''willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it''.

Subsec. (a)(2). Pub. L. 104–294, §201(1)(B), inserted dash after ''thereby obtains'', redesignated remainder of par. (2) as subpar. (A), and added subpars. (B) and (C).

Subsec. (a)(3). Pub. L. 104–294, §201(1)(C), inserted ''nonpublic'' before ''computer of a department or agency'', struck out ''adversely'' after ''and such conduct'', and substituted ''that use by or for the Government of the United States'' for ''the use of the Government's operation of such computer''.

Subsec. (a)(4). Pub. L. 104–294, §201(1)(D), substituted ''protected computer'' for ''Federal interest computer''

and inserted ''and the value of such use is not more than $5,000 in any 1-year period'' before semicolon at end.

Subsec. (a)(5). Pub. L. 104–294, § 201(1)(E), inserted par. (5) and struck out former par. (5) which related to fraud in connection with computers in causing transmission of program, information, code, or command to a computer or computer system in interstate or foreign commerce which damages such system, program, information, or code, or causes a withholding or denial of use of hardware or software, or transmits viruses which causes damage in excess of $1,000 or more during any one-year period, or modifies or impairs medical examination, diagnosis, treatment or care of individuals.

Subsec. (a)(5)(B)(ii)(II)(bb). Pub. L. 104–294, § 604(b)(36)(A), which directed insertion of ''or'' at end of subsec., could not be executed because no subsec. (a)(5)(B)(ii)(II)(bb) existed subsequent to amendment by Pub. L. 104–294, § 201(1)(E). See above.

Subsec. (a)(7). Pub. L. 104–294, § 201(1)(F), added par. (7).

Subsec. (c)(1). Pub. L. 104–294, § 201(2)(A), substituted ''under this section'' for ''under such subsection'' in subpars. (A) and (B).

Subsec. (c)(1)(B). Pub. L. 104–294, § 604(b)(36)(B), struck out ''and'' after semicolon at end.

Subsec. (c)(2)(A). Pub. L. 104–294, § 201(2)(B)(i), inserted '', (a)(5)(C),'' after ''(a)(3)'' and substituted ''under this section'' for ''under such subsection''.

Subsec. (c)(2)(B). Pub. L. 104–294, § 201(2)(B)(iii), added subpar. (B). Former subpar. (B) redesignated (C).

Subsec. (c)(2)(C). Pub. L. 104–294, § 201(2)(B)(iv), substituted ''under this section'' for ''under such subsection'' and inserted ''and'' at end.

Pub. L. 104–294, § 201(2)(B)(ii), redesignated subpar. (B) as (C).

Subsec. (c)(3)(A). Pub. L. 104–294, § 201(2)(C)(i), substituted ''(a)(4), (a)(5)(A), (a)(5)(B), or (a)(7)'' for ''(a)(4) or (a)(5)(A)'' and ''under this section'' for ''under such subsection''.

Subsec. (c)(3)(B). Pub. L. 104–294, § 201(2)(C)(ii), substituted ''(a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7)'' for ''(a)(4) or (a)(5)'' and ''under this section'' for ''under such subsection''.

Subsec. (c)(4). Pub. L. 104–294, § 201(2)(D), struck out par. (4) which read as follows: ''a fine under this title or imprisonment for not more than 1 year, or both, in the case of an offense under subsection (a)(5)(B).''

Subsec. (d). Pub. L. 104–294, § 201(3), inserted ''subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of'' before ''this section'' in first sentence.

Subsec. (e)(2). Pub. L. 104–294, § 201(4)(A)(i), substituted ''protected'' for ''Federal interest'' in introductory provisions.

Subsec. (e)(2)(A). Pub. L. 104–294, § 201(4)(A)(ii), substituted ''that use by or for the financial institution or the Government'' for ''the use of the financial institution's operation or the Government's operation of such computer''.

Subsec. (e)(2)(B). Pub. L. 104–294, § 201(4)(A)(iii), added subpar. (B) and struck out former subpar. (B) which read as follows: ''which is one of two or more computers used in committing the offense, not all of which are located in the same State;''.

Subsec. (e)(8), (9). Pub. L. 104–294, § 201(4)(B)–(D), added pars. (8) and (9).

Subsec. (g). Pub. L. 104–294, § 604(b)(36)(C), substituted ''violation of this section'' for ''violation of the section''.

Pub. L. 104–294, § 201(5), struck out '', other than a violation of subsection (a)(5)(B),'' before ''may maintain a civil action'' and substituted ''involving damage as defined in subsection (e)(8)(A)'' for ''of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb)''.

Subsec. (h). Pub. L. 104–294, § 604(b)(36)(D), substituted ''subsection (a)(5)'' for ''section 1030(a)(5) of title 18, United States Code'' before period at end.

1994—Subsec. (a)(3). Pub. L. 103–322, § 290001(f), inserted ''adversely'' before ''affects the use of the Government's''.

Subsec. (a)(5). Pub. L. 103–322, § 290001(b), amended par. (5) generally. Prior to amendment, par. (5) read as follows: ''intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby—

''(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

''(B) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or''.

Subsec. (c)(3)(A). Pub. L. 103–322, § 290001(c)(2), inserted ''(A)'' after ''(a)(5)''.

Subsec. (c)(4). Pub. L. 103–322, § 290001(c)(1), (3), (4), added par. (4).

Subsec. (g). Pub. L. 103–322, § 290001(d), added subsec. (g).

Subsec. (h). Pub. L. 103–322, § 290001(e), added subsec. (h).

1990—Subsec. (a)(1). Pub. L. 101–647, § 3533, substituted ''paragraph y'' for ''paragraph r''.

Subsec. (e)(3). Pub. L. 101–647, § 1205(e), inserted ''commonwealth,'' before ''possession or territory of the United States''.

Subsec. (e)(4)(G). Pub. L. 101–647, § 2597(j)(2), which directed substitution of a semicolon for a period at end of subpar. (G), could not be executed because it ended with a semicolon.

Subsec. (e)(4)(H), (I). Pub. L. 101–647, § 2597(j), added subpars. (H) and (I).

1989—Subsec. (e)(4)(A). Pub. L. 101–73, § 962(a)(5)(A), substituted ''an institution,'' for ''a bank''.

Subsec. (e)(4)(C) to (H). Pub. L. 101–73, § 962(a)(5)(B), (C), redesignated subpars. (D) to (H) as (C) to (G), respectively, and struck out former subpar. (C) which read as follows: ''an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;''.

1988—Subsec. (a)(2). Pub. L. 100–690 inserted a comma after ''financial institution'' and struck out the comma that followed a comma after ''title 15''.

1986—Subsec. (a). Pub. L. 99–474, § 2(b)(2), struck out last sentence which read as follows: ''It is not an offense under paragraph (2) or (3) of this subsection in the case of a person having accessed a computer with authorization and using the opportunity such access provides for purposes to which such access does not extend, if the using of such opportunity consists only of the use of the computer.''

Subsec. (a)(1). Pub. L. 99–474, § 2(c), substituted ''or exceeds authorized access'' for '', or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend''.

Subsec. (a)(2). Pub. L. 99–474, § 2(a), (c), substituted ''intentionally'' for ''knowingly'', substituted ''or exceeds authorized access'' for '', or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend'', struck out ''as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.),'' after ''financial institution,'', inserted ''or of a card issuer as defined in section 1602(n) of title 15,'' and struck out ''or'' appearing at end.

Subsec. (a)(3). Pub. L. 99–474, § 2(b)(1), amended par. (3) generally. Prior to amendment, par. (3) read as follows: ''knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation;''.

Subsec. (a)(4) to (6). Pub. L. 99–474, § 2(d), added pars. (4) to (6).

Subsec. (b). Pub. L. 99–474, §2(e), struck out par. (1) designation and par. (2) which provided a penalty for persons conspiring to commit an offense under subsec. (a).

Subsec. (c). Pub. L. 99–474, §2(f)(9), substituted ''(b)'' for ''(b)(1)'' in introductory text.

Subsec. (c)(1)(A). Pub. L. 99–474, §2(f)(1), substituted ''under this title'' for ''of not more than the greater of $10,000 or twice the value obtained by the offense''.

Subsec. (c)(1)(B). Pub. L. 99–474, §2(f)(2), substituted ''under this title'' for ''of not more than the greater of $100,000 or twice the value obtained by the offense''.

Subsec. (c)(2)(A). Pub. L. 99–474, §2(f)(3), (4), substituted ''under this title'' for ''of not more than the greater of $5,000 or twice the value obtained or loss created by the offense'' and inserted reference to subsec. (a)(6).

Subsec. (c)(2)(B). Pub. L. 99–474, §2(f)(3), (5)–(7), substituted ''under this title'' for ''of not more than the greater of $10,000 or twice the value obtained or loss created by the offense'', ''not more than'' for ''not than'', inserted reference to subsec. (a)(6), and substituted ''; and'' for the period at end of subpar. (B).

Subsec. (c)(3). Pub. L. 99–474, §2(f)(8), added par. (3).

Subsec. (e). Pub. L. 99–474, §2(g), substituted a dash for the comma after ''As used in this section'', realigned remaining portion of subsection, inserted ''(1)'' before ''the term'', substituted a semicolon for the period at the end, and added pars. (2) to (7).

Subsec. (f). Pub. L. 99–474, §2(h), added subsec. (f).

EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107–296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

TRANSFER OF FUNCTIONS

For transfer of the functions, personnel, assets, and obligations of the United States Secret Service, including the functions of the Secretary of the Treasury relating thereto, to the Secretary of Homeland Security, and for treatment of related references, see sections 381, 551(d), 552(d), and 557 of Title 6, Domestic Security, and the Department of Homeland Security Reorganization Plan of November 25, 2002, as modified, set out as a note under section 542 of Title 6.

REPORTS TO CONGRESS

Section 2103 of Pub. L. 98–473 directed Attorney General to report to Congress annually, during first three years following Oct. 12, 1984, concerning prosecutions under this section.

§ 1031. Major fraud against the United States

(a) Whoever knowingly executes, or attempts to execute, any scheme or artifice with the intent—

(1) to defraud the United States; or

(2) to obtain money or property by means of false or fraudulent pretenses, representations, or promises,

in any grant, contract, subcontract, subsidy, loan, guarantee, insurance, or other form of Federal assistance, including through the Troubled Asset Relief Program, an economic stimulus, recovery or rescue plan provided by the Government, or the Government's purchase of any troubled asset as defined in the Emergency Economic Stabilization Act of 2008, or in any procurement of property or services as a prime contractor with the United States or as a subcontractor or supplier on a contract in which there is a prime contract with the United States, if the value of such grant, contract, subcontract, subsidy, loan, guarantee, insurance, or other form of Federal assistance, or any constituent part thereof, is $1,000,000 or more shall, subject to the applicability of subsection (c) of this section, be fined not more than $1,000,000, or imprisoned not more than 10 years, or both.

(b) The fine imposed for an offense under this section may exceed the maximum otherwise provided by law, if such fine does not exceed $5,000,000 and—

(1) the gross loss to the Government or the gross gain to a defendant is $500,000 or greater; or

(2) the offense involves a conscious or reckless risk of serious personal injury.

(c) The maximum fine imposed upon a defendant for a prosecution including a prosecution with multiple counts under this section shall not exceed $10,000,000.

(d) Nothing in this section shall preclude a court from imposing any other sentences available under this title, including without limitation a fine up to twice the amount of the gross loss or gross gain involved in the offense pursuant to 18 U.S.C. section 3571(d).

(e) In determining the amount of the fine, the court shall consider the factors set forth in 18 U.S.C. sections 3553 and 3572, and the factors set forth in the guidelines and policy statements of the United States Sentencing Commission, including—

(1) the need to reflect the seriousness of the offense, including the harm or loss to the victim and the gain to the defendant;

(2) whether the defendant previously has been fined for a similar offense; and

(3) any other pertinent equitable considerations.

(f) A prosecution of an offense under this section may be commenced any time not later than 7 years after the offense is committed, plus any additional time otherwise allowed by law.

(g)(1) In special circumstances and in his or her sole discretion, the Attorney General is authorized to make payments from funds appropriated to the Department of Justice to persons who furnish information relating to a possible prosecution under this section. The amount of such payment shall not exceed $250,000. Upon application by the Attorney General, the court may order that the Department shall be reimbursed for a payment from a criminal fine imposed under this section.

(2) An individual is not eligible for such a payment if—

(A) that individual is an officer or employee of a Government agency who furnishes information or renders service in the performance of official duties;

(B) that individual failed to furnish the information to the individual's employer prior to furnishing it to law enforcement authorities, unless the court determines the individual has justifiable reasons for that failure;

(C) the furnished information is based upon public disclosure of allegations or transactions in a criminal, civil, or administrative hearing, in a congressional, administrative, or GAO report, hearing, audit or investigation, or from the news media unless the person is the origi-

Appendix B

Revised Recommendation of the Substantive Provisions Work Group

November 19, 2021

Jody R. Westby, Gene M. Smith, Dennis Kelly & Betty Shave

TO: Michele L. Timmons, Chair, ULC Cybercrime Study Committee

FROM: Work Group Members Jody R. Westby, Gene M. Smith, Dennis Kelly & Betty Shave

RE: Revised Recommendation of the Substantive Provisions Work Group

DATE: November 19, 2021

The Substantive Provisions Work Group held several discussions individually and collectively since the last ULC Cybercrime Study Committee meeting on October 26, 2021, to discuss the presentations and comments at the meeting. Based on those discussions and comments, the Work Group has revised its prior recommendation on substantive provisions. The Work Group unanimously proposes the following revised recommendation:

Cybercriminal activity has risen to historic levels, and it is a certainty that state and local law enforcement will have to take on an increasing number of cybercriminal investigations to assist their citizens. Federal cyber investigators are overwhelmed and frequently have to turn away cybercrime cases that meet the threshold for federal jurisdiction, simply because they have no available resources. Investigation assistance is frequently based on the commonality of substantive criminal provisions. Most U.S. states do not have cybercrime laws that address cyber native cybercrimes. Thus, if U.S. state laws are not fully harmonized with federal and international cybercrime laws, states will receive less assistance in cybercrime investigations and citizens will be at risk. The Substantive Provisions Work Group believes that harmonized cybercrime laws for cyber native crimes at the state, federal, and international levels is crucial for states to obtain assistance from each other, the federal government, and other countries.

The Study Committee recognizes the need for procedural provisions at the state level to facilitate cybercrime investigations and prosecutions. However, procedural provisions require underlying substantive provisions; if states do not have harmonized substantive cybercrime provisions, their procedural provisions alone will not be an adequate mechanism for assistance of cyber native crimes.

The Study Committee recognizes the importance of substantive provisions that ensure the confidentiality, integrity, and availability (CIA) of computer systems and data. The principle of CIA is the foundation of information security programs, and therefore, is appropriate when considering substantive cybercrime provisions. After reviewing various legal frameworks, the Study Committee recommends that certain provisions of the Budapest Convention on Cybercrime Titles 1, 2, and 5 serve as guideposts for state cybercrime substantive and procedural provisions.

Title 1 of the Budapest Convention applies to "Offences against the confidentiality, integrity and availability of computer data and systems." The offenses covered within this title are:

- **Illegal access** – access to the whole or any part of a computer system without right

- **Illegal interception** – the interception, without right, made by technical means of non-public transmissions of computer data to, from, or within a computer system.

- **Data interference** – the damaging, deletion, deterioration, alteration, or suppression of computer data without a right

- **System interference** – the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data

- **Misuse of devices** – (1) the production, sale, procurement for use, import, distribution or otherwise making available of (a) a device, including a computer program, designed for the purpose of committing any of the foregoing offenses, (b) a computer password, access code, or similar data by which the whole or part of a computer system is capable of being accessed, with the intent that it be used to commit any of the offenses above, or (2) the possession of an item referred to in (1) with the intent that it be used to commit any of the offenses above. (Note: provision does not apply to authorized testing or protection of a computer system.)

Title 2 of the Budapest Convention applies to computer-related offenses:

- **Computer-related forgery** – the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic.

- **Computer-related fraud** – the causing of a loss of property to another person by (1) any input, alteration, deletion, or suppression of a computer data, (2) any interference with the functioning of a computer system, with the fraudulent intent of procuring, without right an economic benefit for oneself or another person.

Title 5 of the Budapest Convention applies to ancillary liability and sanctions

- Attempt and aiding or abetting the commission of any of the above offenses.

Summary

The foregoing is intended to serve as a minimum floor for uniform or model (to be determined by the Drafting Committee) state cybercrime laws applicable to cyber native crimes.