Comments received in accordance with the Chair's proposal for the work plan for the period 2018-2021

Reproduced as received
Status: Wednesday, 6 March 2019

The present compilation was prepared in accordance with the Chair's Proposal for the 2018-2021 work plan of the Open-ended intergovernmental expert group meeting on Cybercrime, based on Commission on Crime Prevention and Criminal Justice resolution 26/4,[1] approved by the extended Bureau of the expert group on at its meeting on 26 January 2018, which *inter alia* states that:

> Prior to each IEG meeting, the Secretariat will invite Member States to provide, in writing, comments, good practices, new information, national efforts as well as recommendations regarding the meeting's main topics. Observers will be invited to provide relevant information. The Secretariat will then compile and disseminate the information collected not later than three weeks prior to the meeting.

Participating Observers were invited to submit relevant information through Note Verbale CU 2019/4(A)/DTA/OCB/CSS. Two contributions were received from Masaryk University and from the Anti-Phishing Working Group (APWG).

Institute of Law and Technology, Faculty of Law, Masaryk University

Recent developments – CZ:
The Czech Republic has, with the effect from 1 February 2019, adopted updates to criminal procedure that allow for easier discovery of data and that explicitly lay down procedures for quick-freeze. Further amendments are pending regarding particular procedural arrangements for data and for explicit treatment of data as "assets" under the Code of Criminal Procedure. Currently, data are treated, depending on circumstances, under various procedural regimes and the current and pending amendments are to bring greater unification and procedural efficiency into discovery and use of data as evidence in criminal matters.

The Czech Constitutional Court is in upcoming weeks expected to deliver its decision on constitutional compliance of traffic data retention provisions in the Code of Criminal Procedure and the Telecommunications Act. Data retention obligations had already been taken down by the Constitutional Court, the legislation was then redrafted and now it is being on trial again (also following the decision of the Court of Justice of the European Union regarding the Data Retention Directive).

Mostly important for the Czech criminal law regarding investigation and prosecution of cybercrime is in any case the drafted EU legislation regarding cross-border access to electronic evidence, namely the draft regulation on European Production and Preservation Orders for electronic evidence in criminal matters and the draft directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.

Recently (as of 5 February 2019), the European Commission proposed establishing international negotiations on cross-border access to electronic evidence, necessary to track down dangerous criminals

[1] Available at http://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-to-conduct-a-comprehensive-study-of-the-problem-of-cybercrime2018.html

and terrorists. In particular, the agenda includes negotiations with the U.S. regarding access to digital evidence and negotiations on 2nd additional protocol to the Budapest Treaty.

Suggested noteworthy issues for the meeting agenda – forensic standards:

We have been partly involved, on an expert basis, in the development of the EU regulatory framework regarding cross-border digital discovery. The draft EU legislation (the regulation and the directive) aims at cross-border access to digital evidence that is to date unprecedented in international judicial cooperation. The establishment of this cross-border access to digital evidence is possible namely thanks to very similar standards among the EU Member States regarding principles of criminal procedure, protection of fair trial rights, protection of privacy and personal data etc. Still, the development of this procedural regime required (and still requires), despite relative coherence of national laws, significant efforts of the Commission and the Member States. It all implies, at least 3/3 from our perspective, that establishment of any similar procedural cooperation regarding direct or nearly-direct access to digital evidence amongst nations with mutually less compatible legal environments inevitably has to bring even greater challenges.

To the contrary, different procedural or substantive standards in national criminal laws should not represent an obstacle when it comes to technical means or forensic tools used in actual practice of digital discovery. In other words, while we see the establishment of cross-border access to digital evidence as extremely difficult, establishing common standards for the use of technical and forensic tools should not be burdened by differences in national criminal procedures or other relevant factors such as politics.

In that respect, we suggest the intergovernmental Expert Group considering establishment of a certification scheme, best practice evaluation or a similar labelling agenda for forensic tools and/or forensic procedures. These de facto digital forensic standards already exist and are being commonly accepted by investigators. Giving these standards some kind of international official recognition might, in our opinion, provide for greater efficiency of cross-border cooperation in discovery of digital evidence and greater level of certainty of cooperating judicial bodies when it comes to admissibility and evidentiary value of digital evidence discovered abroad.

Anti-Phishing Working Group

The APWG submits the suggestions discussed in this memoranda to illuminate operational aspects of cybercrime-fighting by industry and non-governmental organizations that may be useful to the Intergovernmental Expert Group (IEG) in the development of policy its recommendations under the Salvadore Declaration of 2010, first, to make the IEG aware of efficiencies in data logistics of cybercrime response that the private sector commands and that the group may not fully appreciate — and, secondly, to prevent the possible formation of law, policies and interpretations thereof that may introduce impedances to exchange of data that industry and NGO sectors routinely capture, exchange and employ for suppressing, responding to and investigating cybercrime.

Institutional Profile

The APWG, founded in 2003 as the Anti-Phishing Working Group, is a US-based NGO operating as a trade association, with more than 2000-member enterprises from a majority of the world's countries. Its mission is to address common problems in responding to and managing Internet-based fraud and other electronically mediated crimes. Noteworthy projects with global constituencies include: the eCrime eXchange (eCX), a clearinghouse to report, archive and exchange machine event data related to the commission of cybercrime, programmatically distributing those data to countercybercrime correspondents worldwide on a 24/7 basis; the STOP. THINK. CONNECT. Messaging Convention (a

universal cybersecurity awareness campaign used by government, NGO and private enterprises worldwide, launched as national campaigns in 21 countries since 2010); founding and annual hosting of the APWG Symposium on Electronic Crime Research, the world's only peer-reviewed research conference dedicated specifically to cybercrime studies; and the APWG/CMU-CyLab phishing redirection pages (an free and openly accessible automated education program that directs credulous computer users who've clicked on links to phishing websites to a warning and education page). Learn more here: https://apwg.org/about-APWG/

Memorandum Summary

APWG writes today to proffer perspectives that may be useful in advancing discussions of assisting law enforcement in the suppression/prevention, investigation and prosecution of cybercrimes, specifically in those operational aspects related to the collection, exchange and archiving of evidentiary data in the formation of cybercrime legal cases. In considering the objectives of the Intergovernmental Expert Group (IEG) — to conduct a study of cybercrime and responses to it by Member States, the international community and the private sector to consider options to strengthen existing and new legal or other responses to it — the APWG's believes its most valuable contribution would be to precisely describe the private sectors' roles in preventing, responding to and investigating cybercrime and its routine use of data in the animation of security applications and forensic routines and, from there, to describe the private sector's needs to most efficiently fulfill those briefs. In this memorandum, we submit discussions of such data's mobility and evidentiary utility in three dimensions:

- The operational character and motivations of evidentiary data exchange by private sector enterprises as addressed in law and regulation;
- The role of data clearinghouses operated by private sector commercial enterprises and non-governmental organizations;
- Delineation of personally identifiable information (PII) and its differentiation from the data which describe the machine events that animate a cybercrime.

Private sector data exchange – and its place in law and regulation

United Nations member states developing law and policy related to evidentiary data collection would do well to consider private industry's roles when setting privacy protections in legislation — which are most often consonant with the member state's justice and commerce ministries. Private industry detects and performs most of the primary investigation on cybercrime events yet is hampered by regulations that inhibit the exchange of useful intermediate investigative data that could detect and/or minimize victimization.

For example, the EU GDPR (EU-2016/679) has limits on the exchange of personally identifying data without explicit permission of the 'identifiable' person, yet the law enforcement GDPR (EU-2016/680) has no such provision since it is expected that law enforcement should not tip off the target of an investigation by requesting the target's consent for use of their data. The law enforcement GDPR is strictly limited to public or treaty-based organizations, so it does not apply to private sector security professionals and cybercrime responders and investigators.

This has led to a decrease in useful investigative data sharing and even the complete stoppage of some investigations, security applications and even long-established preventative routines. Additional sequelae of this demobilization of heretofore available data includes the reduction in the number of

potential cases that could be referred to public sector law-enforcement and the elimination of some important data available to enrich the investigations by public-sector law enforcement.

For that reason, APWG sees wisdom in the language of Recital 19 of the GDPR which states, "The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. . .This Regulation should not, therefore, apply to processing activities for those purposes", leading your correspondent to wonder aloud if some degree of codified exception to privacy and data control law – or perhaps a non-ambiguous, delineated freedom of governed access to the data in question — should be extended to private-sector managers, investigators and data correspondents and their clearinghouses.

APWG is fully aware of the dangers of forging a shibboleth that can be arrogated by impertinent pretenders, but we write here today, in part, to give witness to the dysfunction attendant drafting privacy law and regulation under the assumption that they can address all key constituency's needs through legislative architectures that employ conventional divisions of public and private sectors. The emerging cybercrime management plexus that is working and evolving today can, with some legislative nuance, be cultivated into a vastly more effective force for programmatic suppression of cybercrime by removal of ambiguities and prohibitions that enervate data exchange, an issue we consider in the next segment.

Private Sector Data Clearinghouses

With the advent of cybercrime and other abuses of network resources, the private sector spawned new forms of clearinghouses that record events on the Internet that are associated with all manner of malicious behaviors. (ShadowServer and APWG, for examples, were founded in 2004 and 2003, respectively, and many commercial exchanges were established around the same time frame). These organizations archive data and catalogue them for automated retrieval and processing by computer systems dedicated to detecting, suppressing and investigating cybercrimes.

In all of these clearinghouses, no data that can of itself describe a real personality is purposefully archived or exchanged. The archived data is dedicated to describing and recording precise machine-related, system-level events that are associated with a criminal act on a network, such as the establishment of a counterfeit website purporting to offer the services of a well-known bank at a specific Uniform Resource Locator (URL) network address on the World Wide Web – or the scanning by an automated system of network port numbers associated with email exchange.

The examination, fusion and correlation of these events on the public Internetworks and associated resources provide fundamental event data by which security and forensic applications can block, trace and interpret presaging indicators of cybercrimes — and by which investigators can distill forensic narratives. Even the email addresses and telephone numbers recorded in association with cybercrimes on some clearinghouses are most all fictional or abused, temporarily established resources recruited by the perpetrators for criminal enterprise.

In terms of functional profile, the Internet event data clearinghouses that have formed up are replicating the role of the regional laboratories that collect and report out on flu strains that are collected in World Health Organizations (WHO) annual flu vaccination routines. Although the regional laboratories exchange data of a very personal nature, no personality's privacy is betrayed by the system. At its core, the data exchange protocol is largely secured by the data logistics described in the data exchange protocol. While an imperfect analogy, APWG hopes that considering the cybercrime machine event data clearinghouse as inheritors of this kind of role in society, the IEG's imaginations will be inspired

to recommend policies that would clarify these clearinghouse's breadth of access and action – and redound to the broader mobilization of their data assets.

Machine Event Data vs. Personally Identifiable Information

The kind of data that cybercrime responders routinely seek and exchange are, for example, the logs of a collector server or otherwise compromised server. The log files – which will not contain personally identifiable information – are a great resource in identifying the criminal actors, if not their actual identities.

No operational personnel encountered by APWG ever subscribed to the idea that an unenriched Internet Protocol (IP) network address number (that is recorded in server logs) by itself constitutes personally identifiable information, for example, since they change regularly and identify a *system* not a person.

For this reason and other operational realities that are not well addressed in law and regulation, APWG and its data-exchange correspondents are exploring the policy utility of the term *machine event* data that can be used to describe automatically generated technical background data that can be shared and correlated instantaneously through computer programs. This type of data is automatically generated by networked computers and security systems (such as intrusion detection or firewall devices) when they discover malicious activity. APWG and its members and correspondents do not believe a consent option is required for this type of machine-event data or should be required for this type of machine-event data.

Policies and definitions in law and regulations that would clearly and unambiguously distinguish machine event data from PII could go a long way to discipline discussions around privacy and associated law and regulation and align them with operational realities. APWG believes legislation and regulation should be, at a minimum, evidence based. It the absence of non-ambiguous language distinguishing machine events from PII, many initiatives to preserve the rights and freedoms of citizens can be cause more harm than good for want of clarity and mutual understanding of workaday realities.

Conclusion

APWG proffers these discussions as experience-based frameworks that would be useful for managing the development of new policies or disciplining existing policies to comport with operational realities and needs of the private sector which today leads the fight against cybercrime and retains data of evidentiary utility for law enforcement.

The directors of the APWG invite the IEG to request further information and discussion depending on their discussions at hand and attendant research needs.