The APWG is again honored to provide relevant information related to the main topics of the meeting, i.e., international cooperation and prevention, to the UNODC Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime. The APWG, founded in 2003, has for many years has operated a very large international e-crime data clearinghouse that mediates the exchange of machine-event data related to cybercrimes between private sector stakeholders and public sector law enforcement. Today, that clearinghouse delivers hundreds of millions of records per month in answer to data requests by APWG members.

Over the last 16 years, APWG has witnessed criminals, investigators, responders, and nation state policies evolve in their respective roles and enterprises in cyberspace. Criminals continue to thrive in and redefine the cyberattack landscape, and the global response to mitigate threats, identify, apprehend and prosecute cybercriminals lags behind.

Public sector law enforcement officials have recognized that one of the best practices to mitigate e-crime is though the robust sharing of intelligence on criminal infrastructure: Information sharing has for decades been a vibrant, committed, and growing trust-based collaboration between nation states and private organizations. Over the years, public-sector law enforcement has made both government officials and the public aware that information sharing between private sector and law enforcement is essential.

Those organizations recognize that law enforcement organizations cannot collect, process and share such data alone: they rely heavily on the private sector for data and

APWG 405 Waltham Street (PMB 246) Lexington MA 02421
Unifying the Global Response to Cybercrime

analytic tools. The recently evolving data protection and accessibility landscapes, however, have adversely and profoundly affected information exchanges among parties committed to mitigate cyberattacks and cybercrimes.

The APWG's motivation for submitting this commentary is to broaden committee's understanding of the specific needs of stake-holding partners including industry and NGOs like the APWG who routinely exchange data related directly to active cybercrimes and criminal activities for public safety purposes. In many cases, such exchanges are highly automated, near real-time processes. These processes are atypical uses of data that may fall within a data protection remit. They are misunderstood, misrepresented and incorrectly grouped with commercial interests; as a result, accessibility is encumbered or prohibited and this detrimentally affects public safety interventions.

In this submission, the APWG recommends a universal nomenclature for cybercrime data. If employed, these definitions will facilitate adoption of regulations or directives. APWG also recommends specific data handling authority for private-sector interveners and, finally, recommends the adoption of legal frameworks that would define machine event data as separate and distinguished non-amiguously from PII. The APWG thereafter offers use cases to illustrate the role of industry in suppressing cybercrime and bringing cybercriminals to justice. In so doing, APWG also calls attention to the structural impedances that remain in the law that prevent private-sector stake holders and data curators from providing optimal assistance to their public sector contemporaries.

A Universal Nomenclature for Cybercrime Data

The larger community of stake holding interveners needs to develop a common definition for data that require special handling or treatment. New regulations or directives often have different - or new - definitions for data items that the regulators deem private, sensitive, or otherwise objectionable to allow to be exchanged. For example, the definition of personally identifiable information (PII) varies among EU regulation and many other states. A universally recognized definition for special data can remove the impediments and impedances associated with identifying, for example,

what special data can be shared, how, and for how long and thus allow investigators and law enforcers in multiple states to access these data more efficiently - dramatically improving e-crime mitigation, investigation, victim reduction, and perpetrator apprehension.

Data Handling Authority for Machine Event Data for Private Sector Interveners

Studies show that over 95 percent of internet-based crime is detected and initially investigated not by the public sector bodies, but by private organizations, government funded research projects and commercial concerns, including: the APWG (an anti-cybercrime clearinghouse that mediate exchanges of phishing attack data and data related to abuses of cryptocurrency exchanges); CAIDA (the Center for Applied Internet Data Analysis); Cambridge Cybercrime Center at Cambridge University; commercial reputation data service operators such as Spamhaus and SURBL; and commercial security interests.

When cybercrime data processing is placed into the same category as third-party commercial tracking or personalization services, private-sector cybercrime "first" responders, forensic analysts, and criminal investigators are subject to the same rules as marketing and tracking organizations. Ironically, the very parties who historically work to mitigate cybercrime also work to identify and prevent abuses of special data are encumbered by the same rules and regulations as the commercial enterprises that regulations and directives are attempting to constrain through law.

The language and interpretation of GDPR are a case in point. Law enforcement organizations are afforded access to WHOIS contact data related to registration of domain names. There must be some granularity in assignment of access to this essential forensic data and categories of authorized access must be built unambiguously into the law. Private actors acting in the interest of public safety are feeding public-sector law enforcement with the data (and actionable interpretations thereof) to protect the public. These cybercrime responders and forensic artisans must have a different classification than marketing and tracking enterprises. Private sector investigations in the interest of public safety merit the same access as public sector investigations.

The GDPR offers clarification and guidance exclusively for law enforcement operations and in so doing discounts the communities of cyber investigators and first responders who programmatically exchange data that are used to neutralize cybercrime events before they become damaging to people and enterprises. These communities also provide data, services, and tools that law enforcement and departments of justice worldwide rely upon to identify, apprehend and prosecute cyber attackers and criminals.

Machine Event Data vs. Personally Identifiable Information

The kind of data that cybercrime responders and forensic artisans routinely seek and exchange are, for example, the logs of a web, application or cloud server, or compromised systems. The log files are a great resource in identifying the criminal activities.

For example, the data that APWG archives on its eCrime eXchange system for its members identifies systems and behavior observed at those systems that is associated with fraudulent or criminal enterprise and the network locations of the systems without obtaining or revealing PII. [SEE: Figure 1] APWG eCX data archive is one example of many forms of *un*enriched, network event and machine event data that are used to identify fraud or criminal enterprises.

Investigators and public-sector law enforcement have or can (legally and formally) request access to other data such as Whois records or billing statements to identify the actors.

92490171	2020-03-05T22:56:32+00:00	paypal	50	http://uniqueschools.ie/ui/%3fb409443f35946abb53922beceb9dd0a7	active	2020-03-05T22:56:32+00:00	Edit
92490170	2020-03-05T22:54:00+00:00	uber	90	https://www.ubersearch.co.uk/	inactive	2020-03-05T22:54:01+00:00	Edit
92490169	2020-03-05T22:51:01+00:00	PAYPAL	100	http://annoyingadmission.online/	active	2020-03-05T22:52:02+00:00	Edit
92490168	2020-03-05T22:50:06+00:00	Banco Votorantim S/A	90	http://aumenteseulimitepromo.giize.com/JSHCN-AJDKS-AMVND/SREFY67U/	active	2020-03-05T22:50:15+00:00	Edit
92490167	2020-03-05T22:46:28+00:00	AT&T	100	https://forms.gle/9h16XU6NsN79xEak8	active	2020-03-05T22:46:53+00:00	Edit
92490166	2020-03-05T22:45:11+00:00	AT&T	100	https://docs.google.com/forms/d/e/1FAIpQLSfz0t5pHRhO3B1rJkam-fSsgV8wNaUvMdfmDEzgyEIY1ua6PQ/viewform?usp=pp_url	active	2020-03-05T22:45:29+00:00	Edit
92490165	2020-03-05T22:44:08+00:00	AT&T	100	https://docs.google.com/forms/d/e/1FAIpQLSeS5UJSL7YHM95QUnPyJ5SI1PNmnrIsQmUx63CkD7qf2OaiFg/viewform	active	2020-03-05T22:44:30+00:00	Edit
92490164	2020-03-05T22:41:56+00:00	AT&T	100	https://attrefer.weebly.com/	active	2020-03-05T22:42:19+00:00	Edit
92490163	2020-03-05T22:39:22+00:00	NatWest	100	http://www.exellaedu.com/ajax-load/Natwestonlinebanking.Importantupdatenotificationnwolb/Natwestonlinebanking.Importantupdatenotificationnwolb/index.html/	active	2020-03-05T22:39:22+00:00	Edit
92490162	2020-03-05T22:39:00+00:00	linkedin	90	http://cpcalendars.linkedintoweb.com/	active	2020-03-05T22:39:00+00:00	Edit
92490161	2020-03-05T22:39:00+00:00	linkedin	90	http://cpcontacts.linkedintoweb.com/	active	2020-03-05T22:39:00+00:00	Edit
92490160	2020-03-05T22:26:44+00:00	paypal	50	https://id.38degrees.org.uk/clicks/link/32947/35b69c91-e85a-45ff-a936-db49198bf1f1?url=https://thrivecausemetics.com/tools/emails/click/order-confirmation/1/button/view-order-status?url=https%3A%2F%2Fwww.google.com%2Furl%3Fsa%3Dt%26rct%3Dj%26q%3D%26esrc%3Ds%26source%3Dweb%26cd%3D4%26ved%3D2ahUKEwisu_aG	active	2020-03-05T22:26:44+00:00	Edit

Figure 1: Data table of phishing URL reports in CSV format from APWG eCrime eXchanage, March 5, 2020.

APWG and its data-exchange correspondents see the policy utility of the term *machine event* data, a term that we recommend to all policy development agencies and authorities use to describe automatically generated technical background data that can be shared and correlated instantaneously through computer programs.

Machine event data is automatically generated by networked computers as incidental data required for workaday maintenance and troubleshooting and by security systems (such as intrusion detection or firewall devices) when they discover malicious activity. APWG asks that the International Expert Group consider whether or not a consent option is required - or should be required - for this type of event data.

Policies and definitions in law and regulations that would clearly and unambiguously distinguish machine event data from PII could more precisely frame discussions around privacy and associated law and regulation and align them with operational realities. Legislation and regulation should be, at a minimum, evidence based. It the absence of

APWG 405 Waltham Street (PMB 246) Lexington MA 02421
Unifying the Global Response to Cybercrime

non-ambiguous language distinguishing machine events from PII that prevents the resolution of conflicts between privacy laws and counter-cybercrime efforts by both private and public sectors. Many initiatives to preserve the rights and freedoms of citizens can and do demonstrably cause more harm than good for want of clarity and mutual understanding of workaday realities.

Automated Data Exchanges for Programmatic Security Schemes

Much of the data exchange required to respond persistently and effectively to cybercrime is embedded in security software products developed by industry and installed on computing devices. These software tools are fueled by continually refreshed databases to safeguard users' devices and personal data from new threats as they emerge.

Embedded data exchange routines are a key component of computer security software. Computer security software companies programmatically exchange copies of malware with each other that is routinely recovered from customer machines operated by individuals, as well as networked computers managed by commercial enterprises, to update security software products with the latest data that maximizes those tools efficiency in protecting their users from the very latest threats.

As well, these companies and cybercrime investigators also subscribe to commercial and NGO-managed services and government-sponsored resources that supply such data as malware samples (and abstractions of them expressed as digital fingerprints for quick identification of known malevolent code), attack information, operational data related to cybercrime schemes and events and the network numbers of Internet Protocol (IP) addresses that have been associated with cybercrime and other malevolent or anti-social behavior.

APWG has identified three policy dimensions in which private sector enterprises can be more efficiently utilized in the protection of citizens and the promotion of justice as enforced by public sector agencies and law enforcement. A much more powerful and unified global response to the growing cybercrime threat is at hand if the stake holding

communities, including policy makers at the head of the table, can resolve some fundamental, and unnecessary, conflicts in the engagement of data that is essential for the programmatic and maximally efficient suppression of predictable, everyday cybercrimes.

Those key issues include: the establishment of a common nomenclature for cybercrime data; data handling authority for machine event data for private sector intervenors; and the legal disambiguation of PII and machine event data. The directors of the APWG and trustees of the APWG.EU in Spain have at hand a large community of experts from every stake-holding sector and libraries of relevant research that can be put to the task of resolving the policy and operational collisions that allow cybercrime to grow unchecked today. In that pursuit, do know that APWG is at the committee's disposal.

Pat Cain, Director, APWG

David Piscitello, Director, APWG

Peter Cassidy, Director; Trustee, APWG.EU

ИНФОРМАЦИЯ
о сотрудничестве государств – участников СНГ в сфере противодействия киберпреступности

Сотрудничество государств – участников СНГ и взаимодействие их компетентных органов в противодействии киберпреступлениям является одной из задач в сфере совместного обеспечения правопорядка и безопасности Содружества.

С этой целью в СНГ созданы и функционируют комплексная нормативно-правовая база и организационно-практическая система мер, которые последовательно совершенствуются с учетом изменения обстановки и угроз, исходящих от киберпреступности.

Совместные подходы международного сотрудничества стран СНГ по этому направлению отражены в Концепции сотрудничества государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий, которая 25 октября 2013 года одобрена Решением Совета глав государств СНГ. Концепция определяет принципы, задачи, основные направления, формы и систему обеспечения совместной деятельности, направлена на развитие правовых и организационных основ сотрудничества в борьбе с преступлениями, совершаемыми с использованием информационных технологий.

Для практической реализации концептуальных подходов в этой сфере Решением Совета глав государств СНГ от 16 сентября 2016 года утверждена Программа сотрудничества государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий, на 2016–2020 годы.

Принятие Программы обусловлено необходимостью адекватного реагирования государств – участников СНГ на происходящие изменения видов и способов преступлений, совершаемых с использованием информационных технологий, и реализации неотложных мер совершенствования противодействия им.

Документ нацелен на дальнейшее развитие сотрудничества государств – участников и органов СНГ в борьбе с киберпреступлениями и содержит комплекс организационных, правовых и практических мер, направленных на:

дальнейшее развитие международно-правовой базы сотрудничества государств – участников СНГ;

совершенствование и сближение национального законодательства государств – участников СНГ;

проведение комплексных совместных и/или согласованных межведомственных профилактических, оперативно-разыскных мероприятий и специальных операций;

информационное и научное обеспечение сотрудничества, осуществление взаимодействия в подготовке кадров, повышении квалификации специалистов;

развитие сотрудничества с международными организациями.

10.06.2020 9:48:00 20060909

По результатам выполнения Программы ежегодно готовится доклад главам государств и правительств государств – участников СНГ.

В рамках реализации предусмотренных названной Программой мероприятий по совершенствованию правовой базы сотрудничества в этой сфере 28 сентября 2018 года главами государств подписано Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий.

Соглашение нацелено на обеспечение эффективного предупреждения, выявления, пресечения, раскрытия и расследования преступлений в сфере информационных технологий. В нем унифицирован понятийный аппарат, определены направления и формы взаимного сотрудничества, основными из которых являются:

обмен информацией о готовящихся или совершенных преступлениях в сфере информационных технологий и причастных к ним лицах, а также о формах и методах предупреждения, выявления, пресечения, раскрытия и расследования преступлений в данной сфере;

исполнение запросов о получении информации, которая может способствовать раскрытию преступления, о проведении оперативно-разыскных мероприятий, а также о неотложном обеспечении сохранности компьютерных данных;

планирование и проведение скоординированных мероприятий и операций по противодействию преступлениям в сфере информационных технологий;

оказание содействия в подготовке и повышении квалификации кадров.

Для организации обучения, подготовки, переподготовки, повышения квалификации и стажировки сотрудников компетентных органов Решением Совета министров иностранных дел СНГ от 5 апреля 2019 года федеральному государственному казенному образовательному учреждению высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя» придан статус базовой организации государств – участников СНГ по подготовке кадров в сфере борьбы с преступлениями, совершаемыми с использованием информационных технологий, по образовательным программам высшего образования и дополнительным профессиональным программам.

Для подготовки методологических и прикладных основ согласованных действий в этой сфере 18 апреля 2019 года в вышеназванной базовой организации под эгидой Совета министров внутренних дел государств – участников СНГ проведена Международная научно-практическая конференция на тему «Актуальные проблемы противодействия органов внутренних дел (полиции) государств – участников СНГ преступлениям, совершаемым с использованием информационных технологий».