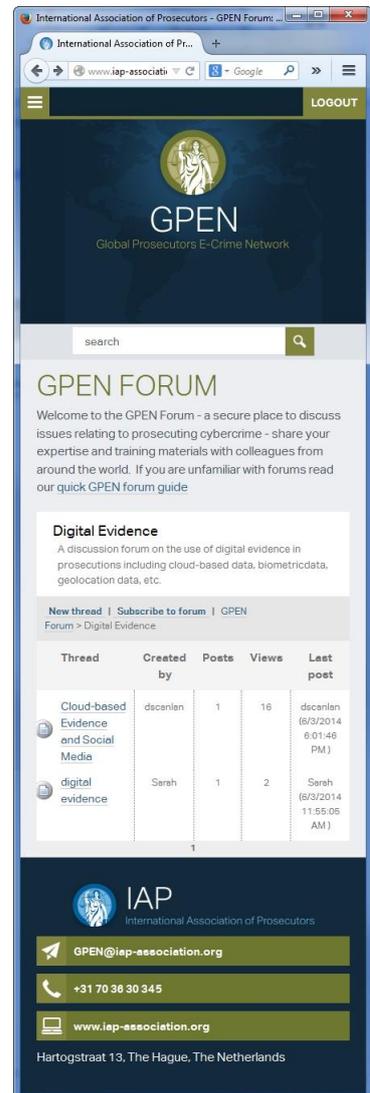




Global Prosecutors E-Crime Network Newsletter Issue 9 June 2014

In this edition read about GPEN's important role in the development of the Commonwealth Cybercrime initiative, the development of Interpol's new complex in Singapore and the arrest of hackers in Columbia who are accused of stealing over \$5 million from individuals bank accounts. This complex and sophisticated crime highlights the issues prosecutors face both finding digital evidence and presenting it in court, so this month the topic focus looks at GPEN's Digital evidence library resources. Continuing this theme, this month's greatest influencer is Daniel Scanlan who has started several very interesting discussions about digital evidence in the GPEN forum, one about the potential implications of biometric data theft and another about the difficulties associated with using Cloud based social network evidence in court. Digital evidence is a fast changing arena and we need your help to keep ahead of the game. Please visit the GPEN forum and join the discussion. There you will meet prosecutors from around the world who can help you with your problems, benefit from your expertise and most importantly forge relationships and contacts that will help improve international cooperation and the effective prosecution of cybercrime. I look forward to meeting you [in the GPEN forum](#).

Sarah Lennard-Brown - GPEN communications team



Join the GPEN community www.iap-association.org/Membership

News

Commonwealth Law Ministers adopt Cybercrime Report

The report of the Commonwealth Working Group of Experts on Cybercrime has been adopted by Law Ministers from the Commonwealth. The report, produced in preparation for the Commonwealth Cybercrime Initiative (CCI), contains recommendations for the development of national strategies and enhanced coordination in efforts to combat cybercrime.



GPEN

Global Prosecutors E-Crime Network



In their endorsement of the report ministers recognised that the Commonwealth is leading the way in the development of international mechanisms to combat cybercrime.

The report was produced by an expert group formed in 2011 which included the International Association of Prosecutors General Counsel Elizabeth Howe and GPEN pioneer Esther George, aimed to review the practical implications of cybercrime in the Commonwealth and identify the most effective means of international cooperation and enforcement.

Colin Nicholls QC, Chair of the Commonwealth Group of Experts on Cybercrime said:

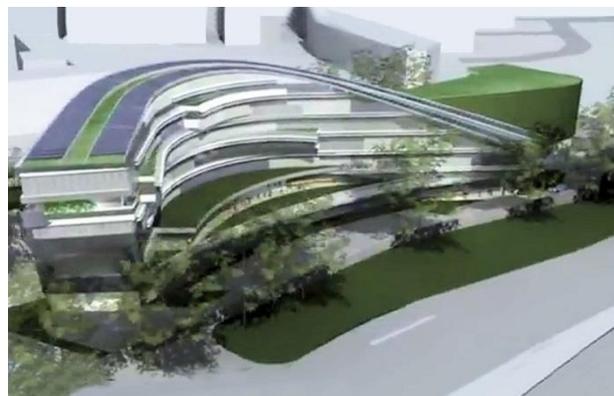
“The report of the group proposes that countries should devise national strategies, which include the development and improvement of laws by using Commonwealth model legislation on computer-related matters. It also proposes the improvement of co-operation in criminal matters between countries, and a strategy to build capacity, such as resources, the expertise of government officials, co-operation with service providers and training of all people concerned including judges, investigators and prosecutors.”

The full report contains several references to the role of GPEN in providing training and networking opportunities.

- Visit the Commonwealth website to download the [report from the Commonwealth Working Group of Experts on Cybercrime](#) PDF 924KB
- For more information about International cooperation [visit the GPEN website](#)

INTERPOL Global Complex for Innovation set for Singapore

INTERPOL have announced that the new ‘Global Complex for Innovation (IGCI) currently being built in Singapore is expected to become operational during 2014. The new IGCI will be a “cutting edge” research and development facility for the identification of crimes and criminals, training and operational support.



The IGCI will focus on the following areas:

- Digital security including a forensic laboratory to support digital crimes investigations, research and analysis services, the development of practical solutions to international cybercrime in collaboration with police, research, academia, public and private sectors.
- Capacity building and training
- Operational and investigative support, identifying and addressing emerging crime threats, providing a platform for disaster victim identification, incident response and major events support and a command and coordination centre.

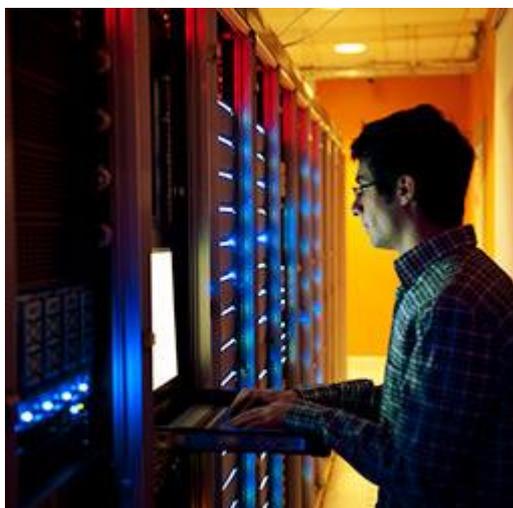
INTERPOL said: “The Global Complex will go beyond the traditional reactive law enforcement model. This new centre will provide proactive research into new areas and latest training techniques. The aim is to give police around the world both the tools and capabilities to confront the increasingly ingenious and sophisticated challenges posed by criminals.”

- For more information about the new IGCI complex in Singapore visit the [INTERPOL website](#)
- Find out more about international cooperation on the [GPEN website](#)

Columbian police arrest alleged bank account hacking thieves

Columbian police have announced the capture of 12 alleged hackers accused of stealing over \$5 million. Three of the suspects are accused of sending emails containing links to a spyware program that recorded the bank details of approximately 15,000 people. Other members of the group are accused of contacting businesses and offering to process some of their employee’s social security payments at a huge discount, the stolen bank account details were then used to make social security payments from the victim’s bank via an online payment system. Victims are thought to have come from eleven different banks in the Caribbean along with the cities of Bogota, Bucaramanga and Cali.

- Find out more about the Columbian arrests on the [InSight Crime website](#)
- Find out more about prosecuting crimes involving malicious software on the [GPEN website](#)



Topic focus – Digital evidence

Gathering digital evidence presents ongoing challenges to both investigators and prosecutors due to fast paced developments in digital hardware, software, social media and communication technology. [The GPEN website library](#) contains a wide range of resources relating to digital evidence retrieval including best practice guides, the most recent of which was published in 2014 by Peter Sommer, and a guide to evidence

gathering and investigation of crimes involving child abuse and safeguarding children. Other resources include a Canadian guide produced in 2006 regarding the presentation of digital evidence in the court room, guides to ethical practice with new technology and a variety of articles and book reviews.

Digital evidence presents opportunities for prosecutors, a recent interactive training program loaded up to the GPEN website; '[Communications data and the proactive Prosecutor](#)' demonstrates how central communications technology can be to all prosecutions.

Digital software and hardware is continually evolving. We would like to expand this to include resources from around the world so please upload your resources to the [GPEN forum](#) and we will try to include them in the library.

Please note: you need to be logged into the [International Association of Prosecutors website](#) using your IAP username and password to access the forum.

Latest activity on the GPEN forum

Daniel Scanlan has started two very interesting discussions this month on the [GPEN forum](#). His first post addressed the issues surrounding the future of crimes involving Identity Theft. He argues that the increasing use of biometrics in the digital world presents a greater potential threat than the theft of passwords. As Daniel says; "When your password gets stolen you can think up a new one. When you're retina scan or fingerprints are stolen, you are compromised for life." He goes on to argue that people who are the victims of digital biometric data theft are at risk of permanent exclusion from many digital services. This discussion was



taken up by both Esther George and Han Moraal, GPEN chairman and Netherlands representative at EUROJUST (European Union Judicial Cooperation Unit). Esther George shared a link with a news story that describes exactly the type of crime anticipated by Daniel which occurred in Israel. Han Moraal questioned whether it was really worse to lose digital biometric data than other important digital data, such as the number of your identity card, to which Daniel gave a very interesting response.

Visit the [GPEN forum](#) to read the full discussion and let us know your experience in this developing prosecution arena.



The second discussion thread started by Daniel Scanlan concerned the use of Cloud-based evidence, especially social networking evidence. Part of Daniel's role is to provide advice, support and training in the use of digital evidence and cybercrime and one of the most common issues people ask him about is the use of Cloud based social networking evidence. One common problem is proving the authenticity of the data to the satisfaction of the court. Daniel describes how they tackle this problem when presenting social networking evidence in the Canadian Courts. This is an area of digital evidence that will increasingly affect all of us. How does your jurisdiction prosecute crimes involving Social Networking evidence? Have you experience of presenting this data in court? Join the discussion on [the GPEN forum](#).

To post on the GPEN forum you need to go to the International Association of Prosecutors (IAP) website and log in with your username and password. Many of you will have an organisational username and password that you can get from your IAP representative. Both organisational and individual members are welcome to join or start conversations on the GPEN forum, it helps us to get to know you if you sign your post with a name or nickname— especially if you are using an organisational login. The GPEN forum is secure, only IAP members can post or read it. If you have forgotten your password click on the "Forgotten password" link on the [IAP website login page](#). If you have forgotten your username email the IAP communications manager at cm@iap-association.org. I look forward to talking to you in the [GPEN forum](#).

Greatest influencers



Each month we introduce an individual who has shown thought leadership within the GPEN community by posting on the forum. This month we profile Daniel Scanlan a Prosecutor from British Columbia in Canada. Daniel has made some very interesting contributions to the GPEN forum on the subject of Digital Evidence and the potential problems presented by the increasing use of bio data as a form of security, (please join the discussion on [the GPEN forum](#) and let us hear your opinion). We are delighted to welcome Daniel to the GPEN forum.

Daniel Scanlan became a prosecutor in 1992 with the federal Department of Justice in Vancouver. In 1999 he moved to Victoria and joined the Attorney General of British Colombia also as a prosecutor.

He said: "My interest in the areas of cybercrime and digital evidence began about 2002 with the prosecution of various child exploitation offenses. To ensure I had an adequate technical background, I attended evening classes in computer science at the University of Victoria. Following

on that training I have received a great deal of valuable experience and information from the highly capable RCMP tech crimes unit. Having practiced in the area for almost 10 years I published a book: "[Digital Evidence in Criminal Law \(2011\)](#)."

My interest in the area arises from the tremendous pace of change as technology drags the justice system behind it. In my view the current digital revolution, particularly in the areas of internet communications and social networking, will be looked back upon by historians as a fundamental societal change as significant as the Industrial Revolution. As this change progresses, new types of evidence appear, new types of offenses are committed and the sheer volume of available information increases geometrically. It is really exciting to be on the leading edge of the changing justice system as it adapts to be a meaningful dispute resolution mechanism for a very changed society. Adapting our centuries-old rules of evidence designed for parchment and paper to each new type of digital evidence is an ongoing challenge.

My current role is with the prosecution support unit. In this role I both prosecute cases involving digital evidence and cybercrime, do any resulting appellate work and provide advice and assistance to other prosecutors on these types of cases. My role also includes teaching other British Columbia prosecutors in this area and providing legal advice to police as to necessary judicial authorizations to obtain the digital evidence they are looking for.



I expect GPEN will be an invaluable part of how prosecutors manage this change. Cybercrime obviously knows no borders so without cooperation and information sharing amongst us our chances of making any significant dent into cybercrime will be diminished. Given the change of pace, if we don't share information, we risk having to each reinvent the wheel ourselves every time something new comes along. The ability to canvas each other's opinions on our forum is going to be a very useful tool as time goes on.

When I am not prosecuting, my retreat is into my hobby of sea kayaking. Sometimes I just go out for the day but once a year I try to go out for a one or two week trip. No technology aboard and I try to get as far away down the British Columbia coast as I can. Success is measured by seeing no one else but the people I am paddling with and not hearing the sound of an internal combustion engine for as long as possible. As a colleague of mine once said: "sometimes you need to sit and think, sometimes you just need to sit..."



Conferences

The Conferences published here are new events that have been added to the GPEN website since the last newsletter was published. For full details of Events relevant to Cyber Crime go to the [Events section of GPEN](#). Please note that to view this information you need to be logged into the website with your International Association of Prosecutors username and password. [Find out how to become a member of the IAP](#).

The International Conference on Digital Security and Forensics (DigitalSec2014)

Date: Tuesday 24 June 2014 - Thursday 26 June 2014

Location: VSB-Technical University of Ostrava, Czech Republic

The event will be held over three days, with presentations delivered by researchers from the international community, including presentations from keynote speakers and state-of-the-art lectures.

Find out more about [DigitalSec 2014](#) on the GPEN website

7th International Conference on Cybercrime Forensics Education and Training

Date: Thursday 10 July 2014 - Friday 11 July 2014

Location: Canterbury Christ Church University, North Holmes Road Campus, Powell Building, Canterbury, United Kingdom,

The conference will include papers, practical workshop proposals, and poster presentations on the following subjects:

- Hacking detection, prevention & prosecution
- Police, University and commercial cybercrime education
- Companies subcontracting forensic analysis
- Ethical, professional and legal issues
- Software tools, Case studies, Career pathways
- Network and mobile communication technologies
- Cybercrime risk management and disaster planning



Find out more about the [CTEC conference](#) on the GPEN website

INTERPOL-Europol Cybercrime Conference

Date: Wednesday 1 October 2014 - Friday 3 October 2014

Location: INTERPOL Global Complex for Innovation (IGCI) in Singapore

The conference is intended to bring together law enforcement and the private sector from across the world to enhance cooperation on cybercrime. The theme of the conference will be 'Cybercrime Investigations – The Full Cycle'.

Find out more about the [INTERPOL conference](#) on the GPEN website

This newsletter is published by the Global Prosecutors E-Crime Network (GPEN) part of the International Association of Prosecutors - Hartogstraat 13, The Hague, The Netherlands
