

PRESENTATION TO BIG DATA CONFERENCE (22 May 2017)
ASSOCIATE PROFESSOR GREGOR URBAS
FACULTY OF BUSINESS, GOVERNMENT AND LAW
UNIVERSITY OF CANBERRA
Email: Gregor.Urbas@canberra.edu.au

Automated Cybercrime Investigations

The example of “Sweetie 2.0”

PRESENTATION OVERVIEW

- Webcam Child Sex Tourism (WCST)
- Sweetie Project
 - Covert investigation by an NGO using a chatbot
- Covert online investigations
- Child grooming sting “operations”
 - “On the Internet, nobody knows you’re a cop”
- Comparative legal analysis
- Australia and the Netherlands
 - Legality and admissibility

WEBCAM CHILD SEX TOURISM

- Webcam Child Sex Tourism (WCST) refers to the use of video-based technologies in order to sexually abuse children in other countries
- It may replace or supplement travel-based Child Sex Tourism (CST), offering an alternative form of engagement for offenders
- Emerging problem in some developing countries e.g. South-East Asia (Philippines) with offenders from both the region and from developed countries (Australia, Canada, US, Europe)
 - “Webcam Child Sex Tourism (WCST) takes place when adults pay or offer other rewards in order to direct and view live streaming video footage of children in another country performing sexual acts in front of a webcam. WCST enables predators to sexually abuse children in other countries with ease and frequency using their Internet-connected personal computers.”
 - Terre des Hommes, *Webcam Child Sex Tourism (Becoming Sweetie: A novel approach to stopping the global rise of Webcam Child Sex Tourism* (published online November 2013):
<http://www.terredeshommes.org/webcam-child-sex-tourism/>

WEBCAM CHILD SEX TOURISM

- **Some features of Webcam Child Sex Tourism (WCST)**
 - Relative safety for offenders – no need to travel to other countries and risk arrest either there or on return to country of origin
 - Can satisfy demand of offenders for child sex experiences going beyond viewing of still images or video i.e. real time participation
 - Can be associated with contact offending e.g. may lead offenders to seek out victims in their own countries or travel for CST
 - Exploits economic and social disadvantage of victims and their families e.g. who may engage in or facilitate the abuse of children
 - May involve criminal networks in the provision of WCST services to paying customers and therefore constitute organised cybercrime
 - Requires significant levels of international co-operation to combat
 - Has so far resulted in only a small number of prosecutions

WEBCAM CHILD SEX TOURISM

TWO DUTCHMEN ARRESTED AT SCHIPHOL AIRPORT FOR WEBCAMSEX WITH CHILDREN

23/05/2016

“Last week at Schiphol Airport two Dutchmen (57 and 59) were arrested on suspicion of online child abuse and child sex tourism. The men were about to leave to Thailand.

The two men are suspected of webcam sex with children, a relatively new phenomenon where children are forced to perform sexual acts for a webcam. The Dutchmen caught the attention of the police during an international investigation into a crime group that offered live streams of sexual abuse of young children in the Philippines. The police investigated dozens of payments of thousands of euros made by the Dutch to the Philippine crime group.”

Terre des Hommes: <https://www.terredeshommes.nl/en/news/two-dutchmen-arrested-schiphol-airport-webcamsex-children>

WEBCAM CHILD SEX TOURISM

- **The “Sweetie” Project**
 - “Terre des Hommes Netherlands researchers spent 10 weeks posing as prepubertal Filipino girls on 19 public chat rooms. During that short period, a total of 20,172 predators from 71 countries committed crimes by soliciting the researchers, whom the predators believed to be minors, for paid webcam sex performances. But 20,172 crimes in a sample of 19 chat rooms likely reflects only a small fraction of the number of crimes actually taking place every day when we consider the US Federal Bureau of Investigation’s estimates that there are 40,000 online chat rooms on which predators lurk. Moreover, WCST takes place on social networking sites, adult webcam sites and online dating sites, in addition to chat rooms. It is likely that WCST takes place tens of thousands of times each day.”
- Terre des Hommes, *Webcam Child Sex Tourism (Becoming Sweetie: A novel approach to stopping the global rise of Webcam Child Sex Tourism)*

WEBCAM CHILD SEX TOURISM

Webcam-child-sex-tourism-te... X +

www.terredeshommes.org/wp-content/uploads/2013/11/Webcam-child-sex-tourism-terre-des-hommes-NL-nov-2013.pd

anzsoc

Page: 50 of 113 Automatic Zoom

[9:22 AM] Candy man: Hi

[9:23 AM] 10 f phil: hi!

[9:23 AM] Candy man: asl?

[9:24 AM] 10 f phil: 10 f philippines

[9:24 AM] 10 f phil: u?

[9:25 AM] Candy man: wow. Im 40/usa/man

[9:25 AM] 10 f phil: 😊

[9:25 AM] Candy man: cam?

[9:26 AM] 10 f phil: what u want to see on cam?

[9:26 AM] Candy man: you

[9:26 AM] Candy man: naked

[9:26 AM] Candy man: if your mother is there she can join.


[9:27 AM] 10 f phil: she not here.

[9:27 AM] 10 f phil: i do for money

[9:27 AM] Candy man: how muuch?

[9:28 AM] 10 f phil: 3 dollar for 10 minute.

[9:28 AM] Candy man: Only if you're sexy



ENG 2:33 AM
CAFR 10/30/2016

WEBCAM CHILD SEX TOURISM

- The introduction of “Sweetie 2.0”
- “While Sweetie 1.0 was extremely successful, one limitation of its design was the human operator. A human operator can only conduct a number of chat conversation at the same time, while real victims receive up to two hundred sex solicitations an hour.
- To counter this problem TdH has developed a more advanced version of Sweetie: Sweetie 2.0. The main difference with Sweetie 1.0 is that Sweetie 2.0 is no longer operated by a human, but is now a fully autonomous artificial intelligence that can engage in a meaningful conversation with a suspect. Unlike human operators, the use of this artificial intelligence is in theory infinitely scalable.”
 - <https://www.terredeshommes.nl/en/sweetie-20-stop-webcam-childsex>

WEBCAM CHILD SEX TOURISM

- The introduction of “Sweetie 2.0”
- “The chat logs are stored and exchanged data are processed per chat to a profile for each chat partner. This profile can ultimately be used to identify repetitive patterns. All chat reports and extracts of chats are logged in a universally accepted standard which facilitates the exchange of cases.
- This will take into account generic storage methods used by various national and international (investigation) agencies such as Interpol and Europol in order to simplify matching with other (online) child abuse cases.”
 - <https://www.terredeshommes.nl/en/publications/full-report-sweetie-20-legal-aspects>

WEBCAM CHILD SEX TOURISM

- Questions posed by the [Sweetie 2.0 Report](#) published by Terre des Hommes in October 2016:
 - “A fundamental criminal law question: is interacting with Sweetie in a sexually charged way even criminal, given that Sweetie is not a person, but a virtual avatar? An answer to this question is important, because if webcam sex tourism with a virtual avatar is not considered criminal, it will be much harder to make the case that the use of Sweetie is an acceptable investigative method.
 - A procedural question: as Sweetie as an investigative tool is so innovative, is it clear whether its use is actually covered by the existing rules of criminal procedure and does its use respect fair trial principles specifically the rules on entrapment?”
 - <https://www.terredeshommes.nl/en/publications/full-report-sweetie-20-legal-aspects>

COVERT ONLINE INVESTIGATIONS

- Problem of a very small window of opportunity to respond to online predators who can groom a child in weeks or even days.
- Covert methods of investigation are justified by the imperative of acting in a pre-emptive manner, recognising the limited opportunities for intervention where children are at serious risk of exploitation and harm – including online exploitation and harms due to contact crimes.
- Covert investigative methods can include:
 - Police posing as children online in chat room “sting operations”
 - Investigators taking over the identity of a key figure in a child exploitation material distribution network
 - Use of “honeypot” sites to identify or warn those seeking such material
 - Creation of online avatars such as “Sweetie” to detect WCST.

COVERT ONLINE INVESTIGATIONS

- Australian courts have generally accepted the use of covert methods in investigating child grooming cases:
 - “The evil to be confronted by this kind of investigation is of high public importance widespread use of the internet gives those disposed to corrupting and sexually exploiting children unprecedented access to vast numbers of potential victims. Such predators would be difficult to detect absent a complaint from an actual victim or an operation such as the present.
 - The Gospel of St Matthew records Christ as condemning those who would corrupt the young ... That, I think reflects the community attitude toward such offences and such offenders. It would support the use of covert operations to detect them in a manner that does not place an actual young person at risk.”
- *R v Stubbs* [2009] ACTSC 63 (26 May 2009), Higgins CJ ruling that the evidence obtained was neither illegal nor improper, thus admissible.
- See for a similar ACT case: *R v Priest* [2011] ACTSC 18 (11 February 2011) and for recent WCST convictions: *R v Goggins* [2014] VCC 1086 (7 July 2014).

COVERT ONLINE INVESTIGATIONS

Criminal Code Act 1995 (Cth), Part 10.6

474.27 Using a carriage service to "groom" persons under 16 years of age

(1) A person (the ***sender***) commits an offence if:

- (a) the sender uses a carriage service to transmit a communication to another person (the ***recipient***); and
- (c) the sender does this with the intention of making it easier to procure the recipient to engage in sexual activity with the sender; and
- (d) the recipient is someone who is, or **who the sender believes to be, under 16 years of age**; and
- (e) the sender is at least 18 years of age.

Penalty: Imprisonment for 12 years.

(2) A person (the ***sender***) commits an offence if:

- (a) the sender uses a carriage service to transmit a communication to another person (the ***recipient***); and
- (c) the sender does this with the intention of making it easier to procure the recipient to engage in sexual activity with another person (the ***participant***); and
- (d) the recipient is someone who is, or who the sender believes to be, under 16 years of age; and
- (e) the participant is someone who is, or who the sender believes to be, at least 18 years of age.

Penalty: Imprisonment for 12 years.

COVERT ONLINE INVESTIGATIONS

Note that s474.28(g) provides

- “it does not matter that the recipient to whom the sender believes the sender is transmitting the communication is a fictitious person represented to the sender as a real person”
- “The wording of the section is plainly wide enough to permit the detection of offenders using the type of subterfuge employed by the police in the present case. Furthermore, the policy of the CPA is to protect children from sexual exploitation. That policy is given effect by s63B(3) which targets people who engage in “grooming” of children for future sexual abuse. Given the policy of the CPA and the purpose of the section there is, in my view, no sensible reason why s63B(3) cannot be used to allow the police to assume the identity of a fictitious child in order to detect offenders engaged in online grooming. Indeed this method of entrapment, the legitimacy of which was conceded by the defence in the present case, is frequently used in the investigation of offences under similar federal and interstate legislation.” (*R v Gedling* [2007] SADC 124 (21 November 2007), Millstead J at [60] in relation to the equivalent South Australian provision).
- “On the Internet, nobody knows you’re a cop”:
<http://www.virtualglobaltaskforce.com/resources/videos/>



On the Internet, nobody knows you're a dog.

LEGAL ANALYSIS

- **Covert online investigation of WCST**
- Webcam-based child sexual exploitation should be amenable to investigation using the same covert methods as apply to other online investigations, including the use of fictional representations of children (where permitted by domestic law).
- However, where a program such as “Sweetie” is used to interact with suspects and collect evidence, it may need additional authorisation as a surveillance device e.g. by means of a warrant issued by a court.
- The automation of “Sweetie 2.0” raises new issues about evidence-gathering e.g. what threshold requirements are there for the use of an automated device not only to observe passively but to engage actively in chat conversations with potential offenders?

LEGAL ANALYSIS

■ Australia

- Grooming of a “fictional” child is still an offence, as long as the defendant believed he was communicating with a child.
- There is no substantive defence of “entrapment” so the admissibility of evidence is assessed in terms of whether it was illegally or improperly obtained and the “public policy” discretion.

■ Netherlands

- Grooming of a fictional child may be considered an attempt to commit a crime, but “attempt to have webcam sex with Sweetie would most likely constitute an absolutely inadequate attempt, which is not punishable regardless of the criminal intent of the alleged perpetrator” (Sweetie 2.0 report).
- Note: This is addressed in new Dutch legislation:
<http://www.thestar.com.my/tech/tech-news/2017/03/06/dutch-consider-tough-new-cybercrime-law/>
- Sufficiently targeted covert operations are not entrapment.

LEGAL ANALYSIS

Circumstances of deployment (e.g. Netherlands)

Covert investigation is generally permissible if the investigator plays an “essentially passive” role i.e. not steering a potential suspect towards commission of a crime but merely allowing him or her the opportunity to demonstrate the predisposition to act criminally.

(Tallon criterion)

“If Sweetie is used in a regular chatroom for users under the age of 18, and her profile resembles that of the majority of minors there, her online presence would abide by this rule [i.e. not significantly altering existing circumstances], if it does not make itself more visible than the mere entering a chatroom with a common-looking chat name.”

LEGAL ANALYSIS

Circumstances of deployment (cont.)

“If, however, Sweetie enters an ‘above 18’ chatroom, already her logging-in is likely to significantly alter the situation. In such cases, the particular assessment of the avatar’s placement will depend among others on the number of real children present there.

While there might be indeed some room to employ the chatbot in online areas intended as ‘adults only’- fora, but demonstrably being used for the webcam prostitution of real children, Sweetie’s appearance in a regular adult chatroom would likely constitute non-targeted entrapment.” (i.e. would not be permissible)

CONCLUSION

- Covert investigative methods have a legitimate role in response to online child sexual offending (as well as other crime types).
 - In some countries, the lawfulness and propriety of police posing as children online have been accepted by courts. In others, legal reforms are in progress to regulate such methods.
 - More sophisticated operations such as “Sweetie 2.0” may raise additional issues such as surveillance devices regulation and the requirements for automated evidence-gathering.
 - Where laws appear to be inadequate, legislative reform should be undertaken to achieve clarity and consistency.
- -- Thank you --