European e-evidence developments

Seminar 'Applying the European Investigation Order'
ERA, Riga | 21 February 2019

Prof. Dr. Gert Vermeulen
t. +32 9 264 69 43
f. +32 9 264 84 94
Gert.Vermeulen@UGent.be

GHENT UNIVERSITY
FACULTY OF LAW

Co-funded by the Justice Programme of the European Union 2014-2020

IRCP Institute for International Research on Criminal Policy
Ghent University

Disclosure slide | background

full-time academic

- international criminal law, EU criminal and JHA policy, cross-border judicial and police cooperation in criminal matters, mutual legal assistance (MLA)
- [other]

data protection professional (since 2013)

- BE: Privacy commissioner, Belgian DPA (Facebook litigation, Yahoo!, Skype)
- EU: member SCG SIS II, Eurodac, VIS, CIS, Europol Cooperation Board, BTLE (Borders, Travel, Law Enforcement subgroup EDPB, preparing EDPB's opinions on the Microsoft Warrant Case and the EC's proposals on e-evidence)
- CoE: T-PD expert (Consultative Committee Convention 108+, 52 countries) for 2nd additional Protocol (e-evidence) to Budapest (Cybercrime) Convention
- ICDPPC: expert group enforcement cooperation, involved in IIOF (UN special rapporteur on the right to privacy's 'Draft legal instrument on government-led surveillace and privacy')

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Structure

jurisdiction and e-evidence: the issue

cross-jurisdictional e-evidence

- Europe
- EU-US

cases and clashes

- Google Spain; Microsoft Warrant; Facebook, Yahoo! & Skype

proposed solutions

- EU level
- CoE level
- [global level: UN special rapporteur | international data access warrant]

competing, legitimate interests at stake

fundamental rights considerations & concerns

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Jurisdiction & e-evidence | the issue

- criminal justice authorities: tradition of cross-border access/MLA based on jurisdictional rules and territory-/sovereignty-based controls and limitations
- unique features of electronic data: increasingly extraterritorial effect
- loss of location (data moving between different services, providers, locations and jurisdictions): what is territorial and what is extraterritorial?
  - possible conflicts of law
  - complexity/fragmentation
  - legal uncertainty for both public authorities and private service providers
  - countries hosting major service providers/data centres: ever-increasing number of requests for e-evidence
- jurisdictional questions often determine the rights and protections that apply (in particular (EU) privacy regulations; GDPR, LED)
- private parties that hold and manage our data increasingly determine whose rules govern and, in key ways, how they are interpreted and applied
  - note: inclusive of so called Over-The-Top (OTT) services, as they are functionally equivalent to more traditional electronic or telecommunication services

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Cross-jurisdictional e-evidence | Europe

current frameworks

- domestic
  - cooperation obligation for telecom and electronic communication providers
- bilateral and multilateral
  - mutual legal assistance (MLA) instruments
  - Budapest Convention, European Investigation Order, …

cross-border access

- formal cooperation between relevant authorities (MLA/EIO) or police-to-police cooperation
- direct cooperation between judicial/law enforcement authority and service provider in another country (voluntary/mandatory)
- direct access from computer

IRCP Institute for International Research on Criminal Policy
Ghent University

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Cross-jurisdictional e-evidence | EU-US

- Electronic Communications Privacy Act (ECPA) | Stored Communications Act (SCA)
- CLOUD Act (Clarifying Lawful Overseas Use of Data)
  - amendment to the SCA to require service providers to "preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."
  - "qualifying" foreign governments get access to records stored in the U.S. that pertain to foreign citizens
- criticism
  - proper safeguards for consumer privacy?
    - discriminatory application to foreign citizens living in the U.S.
    - lack of notice provisions
    - omission of any requirement to obtain a warrant
  - effect on the existing MLA procedures?
  - *quid* GDPR which prohibits the transfer or disclosure of personal data unless pursuant to an MLAT or other international agreement?
  - trans-Atlantic agreement needed

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Cases & clashes

Google Spain case (no primacy of location HQ or data processing)

- EU Court of Justice (13/05/'14): processing of personal data by Google Search is carried out 'in the context of the activities of the establishment in Spain'

Facebook Belgium case (idem)

- BE competence to enforce domestic privacy laws relating to processing of personal data by FB Ireland (on behalf on FB Inc), since carried out in the context of the activities of an establishment on BE territory of the controller (FB Belgium)

Yahoo! Belgium case (primacy of data access over data location) (subscriber information)

- territoriality determined by where data is accessed/received, not where it is located

Skype Belgium case (idem, also for content; lack of office/establishment irrelevant)

- Skype (LU-based) subject to BE jurisdiction by actively participating in the economic life a.o. by language-adapted adverstisment and can be compelled to locally cooperate

Microsoft Warrant case (EU data location-based complication)

- 2nd circuit court '16): law enforcement needs to make a MLA request to foreign government where data is located (Ireland); even so if the crime, victim and target of the investigation are all located in the U.S.
- Supreme Court '18: case declared 'moot' against the backdrop of the Cloud Act

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Proposed solutions | EU level

2016 Council conclusions on criminal justice in cyberspace – Final report

practical measures : improving cooperation

- among judicial authorities
  - within the EU: electronic user-friendly EIO; platform for digital exchanges
  - with the US: dialogue; exchange of best practice; training; information platform
- with service providers (*de facto* main channel),
  e.g. SPOC's, streamlining policies, standardising/reducing forms used in MS

legislative measures (April 2018: 2 EC proposals; MLA "too cumbersome")

- proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters
- proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings
- several issues with legal basis
- more fundamental: judicial cooperation/MLA substituted with compulsary public-private cooperation

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Proposed solutions | CoE level

Budapest (Cybercrime) Convention

- guidance note to accompany art. 18 (production order for subscriber information)
  - requirement mechanism by which law enforcement officials can order "a person in its territory to submit computer data in that person's possession or control"
  - broad jurisdictional reach over extraterritorial providers, without disclaiming government efforts to block such foreign government reach
- initiation draft 2nd additional protocol regarding
  - provisions for more effective MLA (facilitating access to data in foreign, multiple and unknown jurisdictions)
  - provisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information (inclusive of dynamic IP addresses?), preservation requests, and emergency requests
  - clearer framework and stronger safeguards (including data protection requirements, as resulting from Convention 108+) for existing practices of trans-border data access

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Competing, legitimate interests/rights at stake

<u>of states</u>

- right to compell service providers (including OTT) to cooperate re the use of services offered on their territory (i.e. when having an establishment, office or other substantial connection)
- sovereignty of the territory & territoriality of criminal law (clashes; MLA)

<u>of the data subject/person concerned</u>

- right to privacy and data protection
- procedural rights protection

<u>of private companies</u>

- freedom of establishment; right to conduct business/offer services in a global market
- legitimate business interest
- should not be attributed a formal role
  - on behalf of states (in checking whether conditions in requesting/issuing state are fulfilled, whether there are immunities, let alone whether there is sufficient prima facie evidence, …)
  - nor on behalf of the data subject/person concerned (too strongly data location-based interpretation)

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Fundamental rights considerations & concerns

proportionality should be assessed based on the intrusiveness of the data type

- subscriber data (inclusive of dynamic IP addresses) (CoE) or subriber and access data (EU): no offence threshold, can be ordered by prosecutor (no judge required)
- traffic and content data (CoE) or transactional and content data: offence threshold & court/judge production order (preservation order: prosecutor)

data and procedural protection must – again – be maximised (as in MLA)

- in times of 'loss of location', the data storage location (even if relevant from a data protection perspective, especially to shield EU data from US surveillance) seems the least relevant criterion to govern the data protection and procedural rights safeguards that should apply
- work with the combined data protection and procedural rights obligations (double *locus* regime, not just double criminality) of at least
  - as far as subscriber or access data are concerned (or, for mere preservation purposes, of transactional or content data): the country of the requesting/issuing competent authority and the country where the service provider is located
  - as far as transactional or content data are concerned: the country of the requesting/issuing competent authority and the country where the data subject was present whilst using the targeted service (which will be known based on the subscriber/access data)
  - thus putting a person's legitimate expectation of privacy back at the forefront

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Discussion | Q&A

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

www.ircp.org

Contact

Prof. Dr. Gert Vermeulen

t. +32 9 264 69 43
f. +32 9 264 84 94
Gert.Vermeulen@UGent.be

http://www.linkedin.com/in/gert-vermeulen-42b00068

IRCP

Ghent University
Universiteitstraat 4
B – 9000 Ghent

GHENT UNIVERSITY

FACULTY OF LAW AND CRIMINOLOGY

IRCP Institute for International Research on Criminal Policy
Ghent University