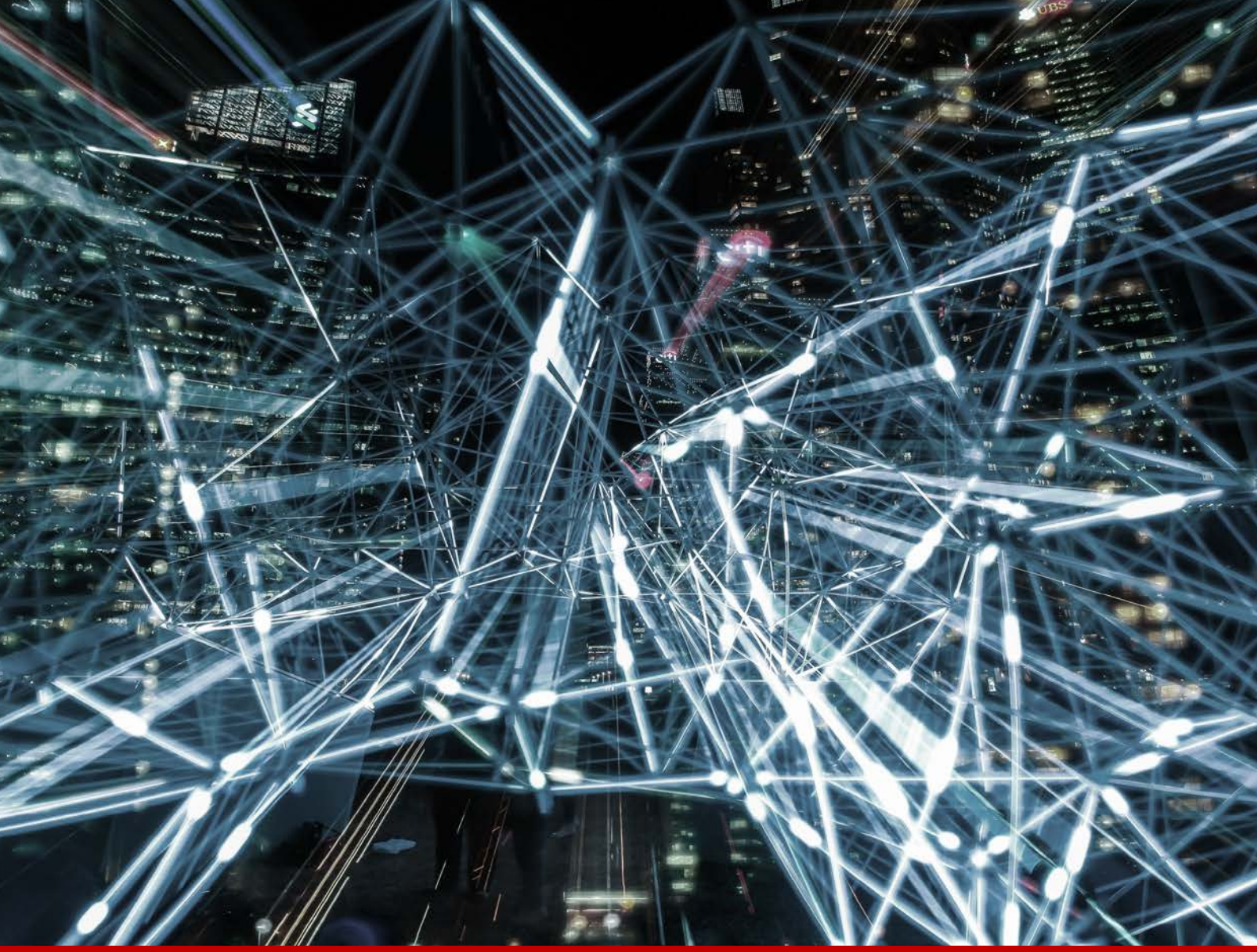


WHOIS behind GDPR?

*25 May is **not** judgment day*

Petillion

For those who have been hiding under a rock for the last two years, the highly anticipated EU General Data Protection Regulation (GDPR) finally came into effect. While many companies have dreaded this day (often afraid of considerable fines or influenced by fearmongering rhetoric), 25 May is unlikely to be the day of judgment.

One thing is for sure: over-extensive compliance efforts by different entities will make it considerably harder for rightsholders to enforce their intellectual property and commercial rights. This is particularly true in an online world, where it will be harder to obtain crucial information from the WHOIS system.

This guide offers practical insight to this issue and highlights the actions needed after 25 May to enforce your rights in a post-GDPR environment.

Content

A. THE GDPR – A BRIEF OVERVIEW

Changes to current framework

- Directly applicable in all 28 Member States
- Extended territorial scope
- Direct obligations for data processors
- Strict conditions for consent
- Stronger rights for data subjects
- No more notification obligation
- Accountability obligations
- Privacy by design and default
- Data transfer obligations
- Notification duty for data breaches
- "One-stop shop" mechanism for cross-border cases
- Higher fines

What is the GDPR?

The General Data Protection Regulation (GDPR) is a new EU regulation which aims to harmonise the rules regarding the protection of personal data in all member states of the European Union.

The GDPR will replace the previous Data Protection Directive (95/46/EC) which has been in effect for more than 20 years. The objective is to adapt the current data protection framework to the rapidly changing digital environment and provide legal certainty for businesses operating across the EU.

As a regulation, the GDPR is directly applicable in all member states without the need for national transposition.

What are the practical implications?

The aim of the GDPR is to promote and facilitate the free flow of data in the EU digital single market. Businesses will only have to comply with a single uniform data protection framework applicable in all member states.

The GDPR imposes new and extensive obligations in relation to accountability, security, lawfulness of the processing, obtaining consent, organisation and procedures, record keeping, international transfers, etc. Additionally, the rights of individual data subjects will be strengthened through the enhancement of the right to information, access and rectification, and through the introduction of the right to be forgotten, data portability and to the restriction of processing.

Businesses and other entities must assess their data processing activities to evaluate if and to what extent the new obligations in the GDPR apply to them. Internal and external data flows must be examined and reconciled with the standards of lawfulness, transparency, purpose limitation and data minimisation.

Is now the time to panic?

No. Various data protection authorities (DPAs) have already indicated that the introduction of the GDPR will be accompanied by dialogue, engagement and cooperation instead of direct enforcement. Many of the principles and obligations of the old regulatory framework are maintained.

B. OVER-COMPLIANCE WITH THE GDPR

In their efforts to achieve compliance with the GDPR, many companies and organisations elect to curtail data collection, processing and disclosure, as they fear high fines and lack common guidelines. They feel that the overall limitation of their data processing activities is easier and provide more certainty than performing the 'difficult' GDPR exercise. This is often due to lack of practical guidance and the existence of several GDPR 'myths'.

Busting GDPR Myths

Myth 1. 25 May is judgment day

Companies and organisations generally perceive 25 May as judgment day for data protection compliance. While the GDPR provides the DPAs with new and more effective tools for investigating and sanctioning infringements, the consensus is to apply the carrot over the stick approach. As a result, DPAs will continue to guide and work with companies and organisations to achieve GDPR compliance and establish a level playing field instead of directly imposing heavy fines.

Myth 2. The GDPR is a radical change to the past

While it is true that the introduction of the GDPR introduces important changes, it does not represent a complete overhaul to the privacy landscape. The GDPR essentially upgrades the existing EU data protection framework which has been in place for more than 20 years. As a result, most of the data processing principles and obligations were already applicable.

Myth 3. The GDPR affects you globally

Whereas the territorial scope of application has been severely extended, the GDPR does not indiscriminately apply outside of Europe. Companies and organisations established outside the European Economic Area (EEA) are not caught by the GDPR unless they target European citizens to offer their products or services, or if they monitor their behaviour inside the EEA.

Myth 4. The GDPR applies to all my data processing activities

The GDPR makes two clear distinctions. First, between the data of natural and legal persons and, second, between identifiable and non-identifiable data. The GDPR's scope of application remains limited to information which identifies or may identify natural persons. As a result, data processing activities concerning the information of legal entities or concerning information which is anonymised are not caught by the GDPR.

Myth 5. Privacy always takes precedence

The principal consideration of the GDPR remains to give data subjects insight in and control over their data. But data protection rights of individuals are not absolute. They must at all times be considered in relation to their function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. As a result, data protection considerations may not unduly restrict other fundamental interests, such as access to

information, the freedom to conduct a business, the protection of IP and consumers, accountability and transparency.

Consequences of over-compliance

The data protection debate often overlooks the importance of available (personal) information for various legitimate purposes, such as law enforcement, consumer protection, (cyber)security and IP enforcement. As a result, over-compliance results in the data protection pendulum swinging too far in the privacy direction, to the detriment of other essential public interests and fundamental rights.

For example, suspected offenders have invoked their privacy rights to escape conviction on the basis of video or photographic evidence. In the fight against counterfeiting, customs authorities also regularly require trademark owners to pay the costs of destruction for counterfeit products, as the disclosure of personal information of the counterfeiting party cannot be obtained. Without this information, it is impossible to make proper investigations and to tackle counterfeit at its source.

The best and arguably the most disturbing example of this worrying trend is the recent confrontation between the GDPR and the registration directory services connected to domain names, also known as WHOIS. Over-compliance with the GDPR threatens to irreversibly affect the availability of essential information related to malicious websites, email addresses and more.

C. POST-GDPR ISSUES: WHOIS

WHOIS?

The WHOIS system contains information on registered domain names, including the identity and contact information of the domain name holder (registrant). For the last 20 years, WHOIS information has been publicly available to all internet users, meaning that everyone could inquire *who is* the holder of a certain domain name within a generic top-level domain (TLD) and what their contact information was.

The WHOIS directory services are coordinated by the Internet Corporation for Assigned Names and Numbers (ICANN), which is the entity responsible for the stable and secure operation of the Internet and its domain name system.

Importance

Swift access to accurate WHOIS data is vital to law enforcement, businesses, consumers, intellectual property owners and cybersecurity service providers.

IP owners depend on WHOIS information in their continuous battle against online infringers. The information is used to identify owners of websites which are hosting illegal content or selling counterfeit products. In order to address cybersquatting or other abusive domain name registrations, trademark owners depend on WHOIS data to identify the malignant registrant and take appropriate action.

Adapting WHOIS to GDPR

Although public access to WHOIS information is of vital importance to IP owners and other legitimate actors, ICANN is currently looking to reform WHOIS, restricting public access in an effort to comply with the principles of the GDPR. The unlimited publication of personal data of individual registrants would raise concerns regarding several aspects of the GDPR, particularly regarding purpose limitation.

ICANN esteems that a 'layered' model of access to WHOIS is necessary, in combination with limited public access to certain data. Under the proposed interim system, parties which are not formally accredited will have access only to a very limited set of publicly available registrant data.

As it stands, public access will be limited to information regarding the registrant's organisation (if applicable), his country state and/or province.

As a result, unaccredited users seeking information on the domain name holder of a particular website will no longer be able to find the name of the registrant, his phone or fax number, or his postal address. Even the genuine email address of the registrant will be concealed behind an anonymised email address or a web form.

Critical issues with the interim WHOIS model

While the implementation of gated access to personal data may be necessary to comply with the principles of the GDPR, the omission of certain important identification and contact information from the public

WHOIS records may prove detrimental to interested parties who fail to get accredited under ICANN's proposed accreditation system.

It is still uncertain who will eventually be **eligible for accreditation** and obtain access to the gated identification and contact information of domain name registrants. Until now, ICANN has specifically mentioned only national law enforcement authorities and IP lawyers. The eventual determination of eligible user groups, accreditation bodies and accompanying codes of conduct is likely to result in confusion and discrimination.

Another problematic aspect of the interim WHOIS model is its **scope of application**. While the GDPR applies only to the data of natural persons, the interim model will apply without making a distinction between natural persons and legal entities. Registrars and registries are permitted to apply the interim model globally, without a connection to the European Economic Area or EU citizens.

Additionally, the **exclusion of the registrant name and email address** from public WHOIS unduly restricts the need for accountability and transparency on the Internet. Expedient access to this information serves all Internet users in identifying and contacting the holder of a domain name to investigate fraud and infringements, to initiate administrative and legal proceedings and to tackle online abuse.

This over-extension of the interim model's scope is not in accordance with ICANN's commitment to "ensure compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible". In its efforts to reaching compliance with the GDPR and avoiding potential fines on May 25, ICANN fails to take due account of other legitimate rights and interests, such as the fundamental right to the protection of IP.

According to the GDPR, the right to the protection of personal data is not an absolute right and must at all times be balanced against other fundamental rights, in accordance with the principle of proportionality. ICANN must thus seek to restore this balance when adopting a final (interim) model.

WHOIS after 25 May

The interim WHOIS accreditation model is far from being implemented. And what is worse than having an unbalanced system is having no system all. In the absence of clear guidance and a set of standards and processes, it is uncertain how various registries and registrars will collect, and make available, WHOIS data now the GDPR's deadline for implementation has lapsed.

Different approaches towards the GDPR's implementation may lead to a fragmented WHOIS system and a potential '**blackout**'. As a result, crucial information risks becoming unavailable to IP owners and interested third parties for an indeterminate period of time.

D. RIGHTS ENFORCEMENT POST-GDPR

ICANN recently introduced the Temporary WHOIS Specification for gTLD registration data, effective as from 25 May. It imposes obligations on gTLD registries and accredited registrars to rapidly achieve compliance with the principles and obligations under the GDPR. The Temporary WHOIS Specification, however, results in over-compliance with the GDPR, to the detriment of rightsholders who depend on WHOIS data to enforce their rights.

'Reasonable' access for legitimate interest purposes

This changed WHOIS environment primarily means that brand owners and other rightsholders will be dependent on a discretionary decision by the applicable registrar or registry on whether to provide the requested non-public registration data. In its Temporary WHOIS Specification, ICANN has introduced the specific requirement that:

> *"Registrar and Registry Operator MUST provide reasonable access to Personal Data in Registration Data to third parties and on the basis of a legitimate interests pursued by the third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Registered Name Holder or data subject pursuant to Article 6(1)(f) GDPR."*

However, by not defining what exactly constitutes 'reasonable access' to personal data and by not providing clear standards for performing the balancing exercise under article 6(1)(f) GDPR, the decision and timing is completely left to the discretion of registrars and registries. This will likely result in a fragmented approach to WHOIS access and the denial of many legitimate disclosure requests.

Lastly, the Temporary WHOIS Specification expressly excludes any third-party beneficiaries, meaning that a rightsholder cannot invoke the violation of the WHOIS Specification directly if reasonable access on the basis of a prevailing legitimate interest is wrongly refused.

WHOIS behind paywall?

Another consequence of gating virtually all registrant information from public WHOIS access is the fact that the incentive for providing privacy or proxy registration services is severely reduced. As personal information is now masked by design, the added value of a service which redacts and substitutes information with that of a service provider is limited. However, many registrars depended on privacy and proxy registration services as an additional way to generate revenue.

It is expected that several of these registrars will now try to put WHOIS disclosure requests behind a paywall in order to make up for this lost revenue. Charged access models could take different forms. Single query requests could require the payment of a fixed one-time fee. Potentially, access could also be provided on a subscription basis, taking into account the legitimate interest of the subscriber for each request. However, such a practice may be seen as being at odds with section 3.3.1. of ICANN's Registrar Accreditation

Agreement which states that accredited registrars shall provide "free public query-based access to up-to-date data concerning all active Registered Names sponsored by Registrar in any gTLD". As a result, free and expedient access to essential information must still be encouraged for legitimate third-party interests.

Impact on UDRP/URS

Brand owners depend on readily accessible WHOIS information to prepare UDRP or URS administrative proceedings against a malignant registrant. Without access to the registrant's name, email and postal address, it becomes more difficult to develop important arguments such as on the language of the complaint, knowledge of the complainant's trademark and the showing of a pattern of bad faith registrations. Additionally, it may no longer be possible to ascertain whether different domain names where registered by the same person to group these multiple domain names in a single complaint.

As it stands, it looks like Complainants will have the possibility to present a "Doe" complaint to the relevant administrative center, such as the WIPO Arbitration and Mediation Center, who will then request the applicable registrar to provide the necessary identification and contact information to complete the required fields of the complaint. A complainant can amend his complaint afterwards, taking into account this new information. ICANN's latest amendments to its Temporary WHOIS Specification specifically provide that:

> *"Complainant's complaint will not be deemed defective for failure to provide the name of the Respondent (Registered Name Holder) and all other relevant contact information required by [the UDRP and URS Rules] if such contact information of the Respondent is not available in registration data publicly available in RDDS or not otherwise known to Complainant. In such an event, Complainant may file a "Doe" complaint and the Provider shall provide the relevant contact details of the Registered Name Holder after being presented with a "Doe" complaint."*

Apart from considerations related to timing and costs, this would mean that proceedings must be initiated 'blindly'. A complainant will be able to evaluate the viability of initiating proceedings only after the complaint has already been filed. In addition, trademark holders are again at the mercy of a disclosure decision by the relevant registrar, many of which are regularly in default from both an accuracy and efficiency perspective.

If you have faced any issue on the collection of WHOIS information, let us know: info@petillion.law.

E. OUTLOOK

Expedited Policy Development Procedure (EPDP)

As the Temporary WHOIS Specification can be maintained for up to one year only, the adoption of this Specification is not the final stop for amending the WHOIS system. For the first time, ICANN's policy development body, the GNSO, has agreed to initiate an EPDP which aims to implement a final interim WHOIS model within 360 days.

Further Community Action

For the implementation of a final interim WHOIS model, ICANN acknowledges that further issues are still outstanding and must be resolved as soon as possible after 25 May. As a result, community discussion will continue with a view to achieving a WHOIS model that deals with the need for (i) unique contact email addresses, (ii) effective access to relevant WHOIS information for good-faith UDRP or URS complaints, (iii) distinguishing between natural and legal persons, (iv) automated access for realistic investigatory cross-referencing needs, and (v) a mandatory and consistent process for access to registration data for users with a legitimate purpose until a balanced system for accreditation and access to gated WHOIS data for those users is implemented. A balanced accreditation and access mechanism must ensure that all interested third parties can obtain expedient access to the necessary information for essential legitimate purposes.

F. ACTION POINTS

1. Advocate for balance

Although the Temporary WHOIS Specification is deficient due to over-compliance with the GDPR, rightsholders and other interested third-parties can still engage in correcting over-compliance with the GDPR in favour of legitimate public and third-party interests.

In this regard, public access to essential WHOIS information serving the public interest, notably the name and email address of the registrant, should be maintained. Additionally, effective access for rightsholders to all relevant WHOIS data must be ensured under the accreditation mechanism, including automated access to assess aggregated ownership and patterns of infringing behaviour.

2. Take action against over-compliant parties

When rightsholders sustain damages due to their inability to enforce their rights in a post-GDPR environment, they should not shy away from taking effective action. Registrars and registries who prevent or delay expedient access to vital information and do not sufficiently take into account legitimate third-party interests can be dealt with in Europe on the basis of a general tort claim and by establishing contributory liability

Contact information

We are members of the Brussels Bar

Offices

GG 126
Guido Gezellestraat 126
1654 Huizingen
Belgium (Europe)

Contact

info@petillion.law
T. +32 2 306 18 60
F. +32 2 306 18 69

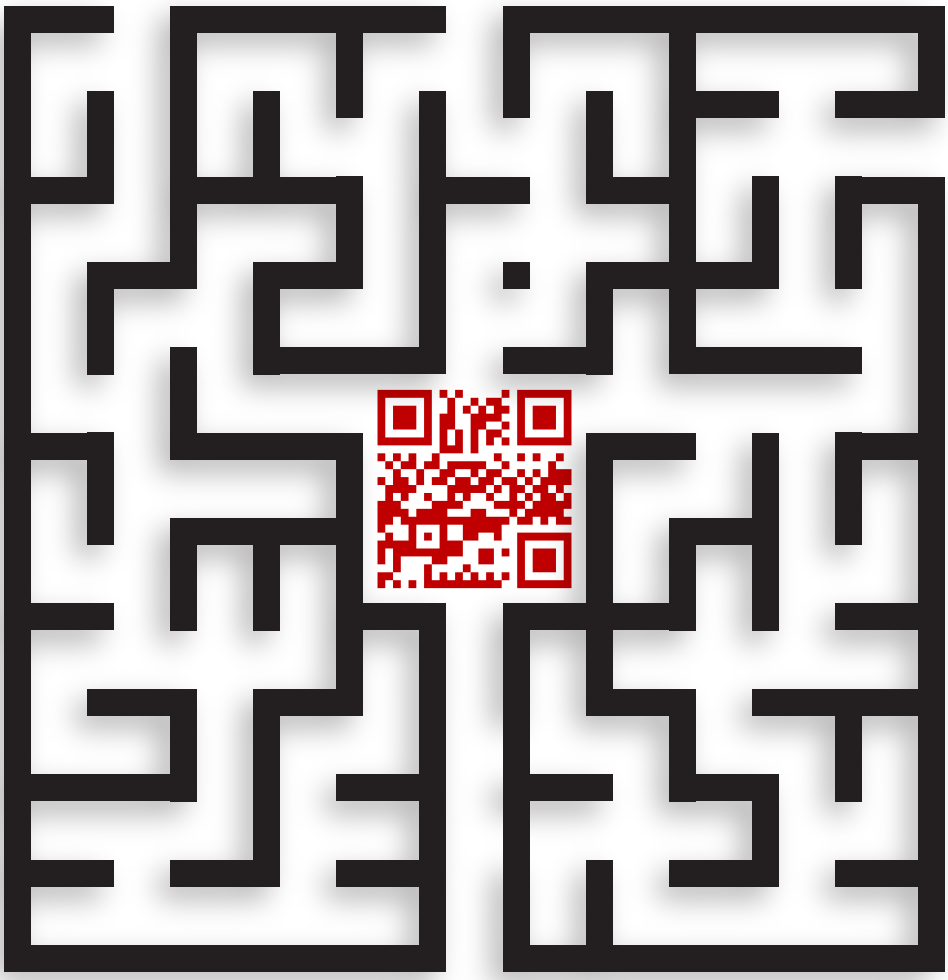
www.petillion.law

Time zone

West Coast	East Coast	London	Petillion	Abu Dhabi	Singapore	Sydney
UTC -8	UTC -5	UTC	UTC +1	UTC +4	UTC +8	UTC +11
PST	EST		CET	GST	SGT	AET

Petillion

Attorneys - Advocaten - Avocats



Your gateway to dispute resolution

www.petillion.law