

Refinement of Legal Specifications in the Lex Programming Language

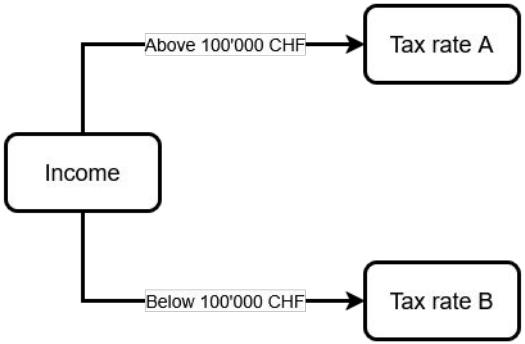
Master's Thesis by Jonas Degelo

Motivation

Motivation for Legal Formalization

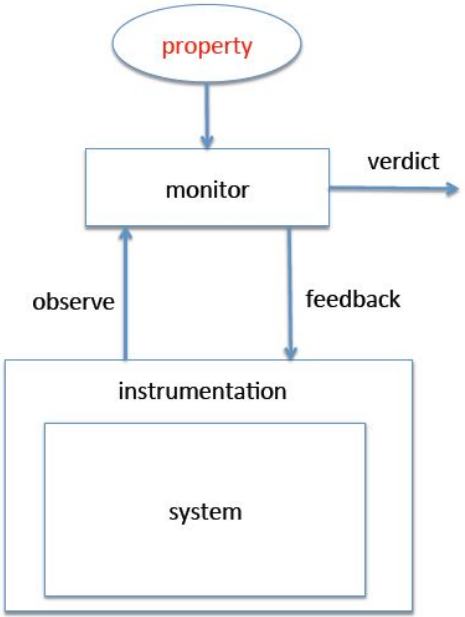
- Illustration of logical structure
- Broader access
- **Automatization**





Formalizing the Law for Runtime Verification

- Runtime Monitoring and **Runtime Enforcement**
  - Monitoring: check for compliance
  - Enforcement: ensure compliance
- State of the art verification tools **require the law to be encoded as logical formulae**
- Direct translation of legal texts to logical formulae is a difficult and error-prone task
- A “good” formalization **maintains readability** and allows for automation



Why is Refinement Needed?

- Writing specifications at **different levels of abstraction**
- Reusability of existing formalizations
- Example:
  - Formalize the GDPR once
  - Adapt it for different services with minimal effort

Preliminaries

- Legal Background
- Refinement of Specifications
- The Lex Programming Language

Legal Background

Vagueness of the Law

The Human Element

- Vagueness is inherent to the law
- Consensus among scholars is that human interpretation cannot be eliminated entirely
- We aim to offer a solution to formalize the logical structure of legal texts
- Ambiguities can be decided by a human and the decisions can be provided as inputs to our system

Logical Structure of the Law

- **Obligations** limit what is allowed
- **Exceptions** specify when some other section of the law does not apply
- Institutional vs. brute facts
  - Brute facts are **“facts of nature”**
    - a person's age, a car’s speed, etc.
  - Institutional facts are **derived from other facts**
    - A person is allowed to vote in Switzerland if they are over 18 and a Swiss citizen
    - “Having the right to vote” is an institutional fact
- **The difference between Institutional and Brute facts can be fluid**
  - Refinement use case

Rules

Example: Building Access

1. To enter the building **authorization is required**

2. **Employees are authorized** to enter the building

3. During time off, Rule 2. does not apply

- Regulative (Obligation) Rule
- Constitutive Rule
- Exception

Refinement of Specifications

Refinement

- Two models of the world
  - A mapping between the two
- Specification A for model 1 and specification B for model 2
- **Specification A refines specification B** if every behavior that is compliant with Specification A, it is compliant with specification B, when mapped to model 2
  - Imagine one specification for C++ and one for x86 assembly

The Lex Programming Language

- Temporal Logic
- Hierarchical Structure
- Events and Types
- Rule Types

Metric First Order Temporal Logic (MFOTL)

First order predicate logic $\phi \wedge \psi,\ \phi \vee \psi,\ \neg\phi,\ P(x),$ etc.



Always	$\Box_I\ \phi$	Historically	$\blacksquare_I\ \phi$
Until	$\phi\ \mathcal{U}_I\ \psi$	Since	$\phi\ \mathcal{S}_I\ \psi$
Next	$\bigcirc_I\ \phi$	Previous	$\bullet_I\ \phi$
Eventually	$\Diamond_I\ \phi$	Once	$\blacklozenge_I\ \phi$

Section Labels




```
law "U.S. Code"

title "26"

title[1] "A"

chapter "1"

chapter[1] "B"

section "III"

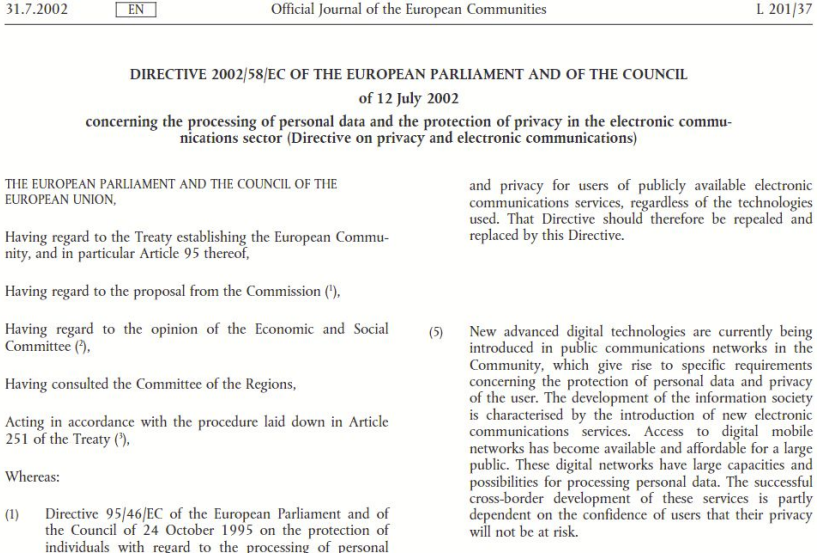
article "121"
```

Lex Code: US Tax Code

[3]

ePrivacy Directive (EU)

Lex Example



31.7.2002 EN Official Journal of the European Communities L 201/37

DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 12 July 2002

concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Having consulted the Committee of the Regions,

Acting in accordance with the procedure laid down in Article 251 of the Treaty (3),

Whereas:

(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal

and privacy for users of publicly available electronic communications services, regardless of the technologies used. That Directive should therefore be repealed and replaced by this Directive.

(5) New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the information society is characterised by the introduction of new electronic communications services. Access to digital mobile networks has become available and affordable for a large public. These digital networks have large capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk.

Event and Type Definitions

epd.lex

```
type person
type purpose is string
type productCategory is string

internal event automatedCommunication
    """ person {receiver} receives an automated message about a
    product or service from category {c} from person {sender} for
    purpose {p}"""
    sender: person
    receiver: person
    p: purpose
    c: productCategory

causable suppressable event automatedCall
    """ person {r} receives an automated call about a product
    or service from category {c} from person {s} for purpose {p}"""
    r: person
    s: person
    p: purpose
    c: productCategory
```

Obligation Rules

epd.lex

```
article "13" "Unsolicited communications"
paragraph "1"

rule "marketing consent requirement"
    whenever
        automatedCommunication(s, r, "marketing", c)
    oblige
        marketingConsent(r, s)
    enforceable suppressing automatedCommunication
```

Article 13

Unsolicited communications

1. The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.

Constitutive Rules

epd.lex

```
rule "automated call communication"
    whenever
        automatedCall(s, r, p, c)
    constitute
        automatedCommunication(s, r, p, c)

rule "fax communication"
    whenever
        fax(s, r, p, c)
    constitute
        automatedCommunication(s, r, p, c)

rule "email communication"
    whenever
        email(s, r, p, c)
    constitute
        automatedCommunication(s, r, p, c)
```

Article 13

Unsolicited communications

1. The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.

ePrivacy Directive (EU)

Exception Rules

epd.lex

```
paragraph "2"

rule "marketing of similar products or services"
    whenever
        obtainedEmailForCategory(r, s, c)
        NOT objectToSimilarEmailMarketing(r, s, c)
    except
        article "13" paragraph "1"
```

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and on the occasion of each message in case the customer has not initially refused such use.

Compiled Lex Code

MFOTL Formula of **`epd.lex`**

```
LET automatedCommunication(_p1 : int, _p2 : int, _p3 : string, _p4 : string) =
    email(_p1, _p2, _p3, _p4)
    ∨ fax(_p1, _p2, _p3, _p4)
    ∨ automatedCall(_p1, _p2, _p3, _p4) IN
LET Exception4(c : string, r : int, s : int)? =
    obtainedEmailForCategory(r, s, c)
    ∧ ¬objectToSimilarEmailMarketing(r, s, c) IN
LET Scope5(r : int)? = isNaturalPerson(r) IN
□[0s,∞) (∀c. ∀r. ∀s. automatedCommunication(s, r, "marketing", c)
            ∧:L ¬Exception4(c, r, s)
            ∧ Scope5(r) →:L marketingConsent(r, s))
```

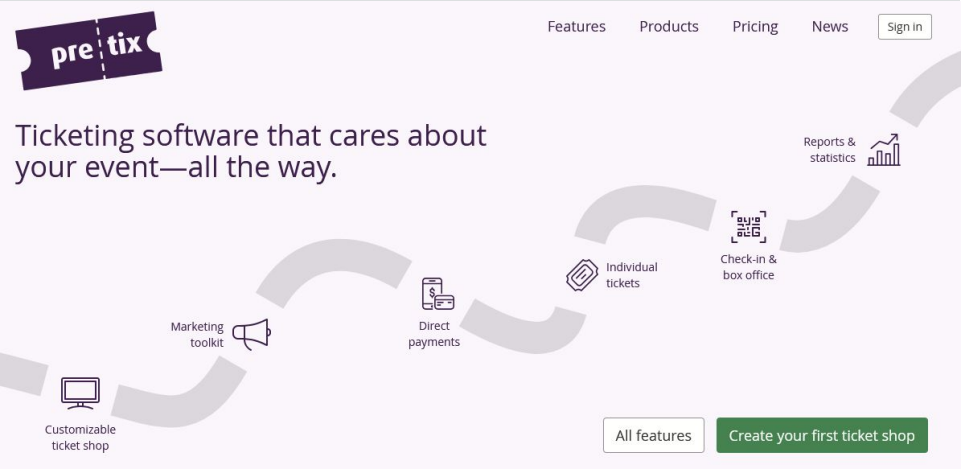
MFOTL Signature of **`epd.lex`**

```
automatedCall(r: int, s: int, p: string, c: string)+-
email(r: int, s: int, p: string, c: string)+-
fax(r: int, s: int, p: string, c: string)+-
isNaturalPerson(s: int)
marketingConsent(r: int, s: int)
objectToSimilarEmailMarketing(r: int, s: int, c: string)
obtainedEmailForCategory(r: int, s: int, c: string)
```

Contributions

- Refinement Rules for Lex
- Established connection be refinement in Lex and refinement in literature
- Implementation of refinement in the Lex compiler
- Case Study applying refinement to the EU's ePrivacy Directive

Pretix



- Open source ticketing platform
- Built with Python & Django
- **Instrumented** with `instrlib` for enforcement of ePrivacy Directive (Article 13)
- **Refined** Article 13 for Pretix

Refining the ePrivacy Directive in Lex for Pretix

Refine Data Types & New Events

epd.rex

```
refine epd

refine type person is string

observable event userGivesConsent
    """ person {s} gives consent to receive automated marketing communication from person {r} """
    r: person
    s: person

observable event userWithdrawsConsent
    """ person {s} withdraws consent to receive automated marketing communication from person {r} """
    r: person
    s: person

observable event over18
    """ person {r} is over 18 years old """
    r: person
```

Refine Concrete Events

Refined and Assumed events (`epd.rex`)

```
rule "refine marketing consent"
    whenever
        (NOT userWithdrawsConsent(r, s)) SINCE userGivesConsent(r, s)
    refine
        marketingConsent(r, s)

assume true objectToSimilarEmailMarketing
assume true isNaturalPerson

assume false fax
assume false automatedCall
```

Replace Obligations with Stronger obligations

Old, weaker rule (**`epd.lex`**)

```
article "13" "Unsolicited communications"
paragraph "1"

rule "marketing consent requirement"
    whenever
        automatedCommunication(s, r, "marketing", c)
    oblige
        marketingConsent(r, s)
    enforceable suppressing automatedCommunication
```

- “New rule” -> “Old rule”
- Lex compiler checks implication using SMT solver

New, stronger rule (**`epd.rex`**)

```
rule "stronger_consent"
    whenever
        automatedCommunication(s, r, "marketing", c)
    oblige
        marketingConsent(r, s)
        over18(r)
    enforceable suppressing automatedCommunication

replace
    strengthen
        article "13" paragraph "1"
    by
        rule "stronger_consent"
```

ePrivacy Directive (EU)

Strengthening or Weakening Constitutive Rules

- **Strengthening** → “(Internal) Event gets emitted **less often**”
  - Constituted event ust be **anti-monotonic**
  - An event is anti-monotonic if it **cannot make a trace more compliant**
- **Weakening** → “(Internal) Event gets emitted **more often**”
  - Constituted event must be **monotonic**
  - An event is monotonic if it **cannot make a trace less compliant**

Strengthening or Weakening Constitutive Rules

Old, weaker rule (`epd.rex`)

```
rule "refine marketing consent"
    whenever
        (NOT userWithdrawsConsent(r, s)) SINCE userGivesConsent(r, s)
    refine
        marketingConsent(r, s)
```

- Refinement of previous refinement
- New rule is more restrictive than old rule
- Lex compiler checks implication
  - Strengthening: “new” -> “old”
  - Weakening: “old” -> “new”
- (Anti)-monotonicity gets checked according to topological ordering of rules

New, stronger rule (`epd-2.rex`)

```
refine rex epd

rule "consent expiration"
    whenever
        ONCE[0, 30d] userGivesConsent(r, s)
        (NOT userWithdrawsConsent(r, s)) SINCE userGivesConsent(r, s)
    constitute
        marketingConsent(r, s)

replace
    strengthen
        rule "refine marketing consent"
    by
        rule "consent expiration"
```

Compiled Lex and Rex MFOTL Formulae

Lex MFOTL Formula of **`epd.lex`**

```
LET automatedCommunication(_p1 : int, _p2 : int, _p3 : string, _p4 : string) =
    email(_p1, _p2, _p3, _p4)
    v fax(_p1, _p2, _p3, _p4)
    v automatedCall(_p1, _p2, _p3, _p4) IN
LET Exception4(c : string, r : int, s : int)? =
    obtainedEmailForCategory(r, s, c)
    ∧ ¬objectToSimilarEmailMarketing(r, s, c) IN
LET Scope5(r : int)? = isNaturalPerson(r) IN
□[0s,∞) (∀c. ∀r. ∀s. automatedCommunication(s, r, "marketing", c)
           ∧:L ¬Exception4(c, r, s)
           ∧ Scope5(r) →:L marketingConsent(r, s))
```

- Assumed events
- Refined (and strengthened) consent
- (Strengthened) Obligation

Rex MFOTL Formula **`epd-2.rex`**

```
LET automatedCall(_p45 : string, _p46 : string, _p47 : string, _p48 : string) = ⊥ IN
LET fax(_p49 : string, _p50 : string, _p51 : string, _p52 : string) = ⊥ IN
LET isNaturalPerson(_p53 : string) = ⊤ IN
LET marketingConsent(_p57 : string, _p58 : string) =
    ♦[0s,30d+0s] userGivesConsent(_p57, _p58)
    ∧ (¬userWithdrawsConsent(_p57, _p58) S[0s,∞) userGivesConsent(_p57, _p58)) IN
LET objectToSimilarEmailMarketing(_p54 : string, _p55 : string, _p56 : string) = ⊤ IN
LET Exception4(c : string, r : string, s : string)? =
    obtainedEmailForCategory(r, s, c) ∧ ¬objectToSimilarEmailMarketing(r, s, c) IN
LET automatedCommunication(_p41 : string, _p42 : string, _p43 : string, _p44 : string) =
    email(_p41, _p42, _p43, _p44)
    v fax(_p41, _p42, _p43, _p44)
    v automatedCall(_p41, _p42, _p43, _p44) IN
LET Scope5(r : string)? = isNaturalPerson(r) IN
□[0s,∞) (∀c. ∀r. ∀s. automatedCommunication(s, r, "marketing", c)
    ∧:L ¬Exception4(c, r, s) ∧ Scope5(r)
    →:L marketingConsent(r, s) ∧ over18(r))
```

Compiled Lex and Rex MFOTL Signatures

Lex MFOTL Signature of **`epd.lex`**

```
automatedCall(r: int, s: int, p: string, c: string)+-
email(r: int, s: int, p: string, c: string)+-
fax(r: int, s: int, p: string, c: string)+-
isNaturalPerson(s: int)
marketingConsent(r: int, s: int)
objectToSimilarEmailMarketing(r: int, s: int, c: string)
obtainedEmailForCategory(r: int, s: int, c: string)
```

Rex MFOTL Signature of **`epd-2.rex`**

```
email(r: string, s: string, p: string, c: string)+-
obtainedEmailForCategory(r: string, s: string, c: string)
over18(r: string)
userGivesConsent(r: string, s: string)
userWithdrawsConsent(r: string, s: string)
```

- Only non-internal events are part of the signature
- **Assumed** and **refined** events are internalized
- **New events** are added to the signature

Future Work

Future Work

- Larger Case Study
  - Formalize larger specifications
  - Refine for more aspects of a system
- A package management infrastructure for Lex Refinement
  - Repository of existing Lex formalizations

Notes

- Lex does not attempt to automatically infer the meaning of the law
- LLMs could assist with semi-automatic formalization
  - Recent bachelor's thesis (generating Lex code from natural language)
  - Some amount of human interpretation will very likely always be needed
- Lex aims to improve auditing process
- Refinement in Lex allows for auditing at different layers
  - Reducing complexity at each layer

References

[1] A Tutorial on Runtime Verification - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/An-overview-of-the-runtime-verification-process_fig1_303161021 [accessed 9 Jun 2025]

[2] https://www.law.cornell.edu/uscode/text/26/121

[3] https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng

[4] https://www.vecteezy.com/vector-art/534940-gdpr-general-data-protection-regulation-icon-line-style

[5] https://pretix.eu

Implementation

Compilation Pipeline

