# Text and Pretext on the Internet: Recognizing Problematic Communications

**Carole E. Chaski, PhD**
**Raye Croghan**
**ALIAS Technology LLC**
**http://www.aliastechnology.com**
**Institute for Linguistic Evidence Inc**
**http://www.LinguisticEvidence.org**

**ABSTRACT**
A key feature of human linguistic ability, the ability to recognize members of our linguistic community and text types, is essential for safety on the Internet, but this ability is immature in minors, hampered by the rarity of problematic text types in everyday life, and hindered by the keyboard dilemma. ALIAS (Automated Linguistic Identification and Assessment System) provides a working system for classifying texts, assessing threats and determining authorship and has already been admitted as scientific evidence without restrictions into American courts. We propose extensions to ALIAS to recognize texts and pretexts in all forms of predatory electronic communication.

**Keywords**
Forensics, identification, parental controls, filtering.

**Functional Goals**
Limit harmful contact between adults and minors,
Limit harmful contact between minors,
Prevent harassment, unwanted solicitation, and bullying of minors on the Internet,
Other – authorship identification and threat assessment.

## THE PROBLEM OF TEXT AND PRETEXT ON THE NET

### Linguistic Recognition As a Safety Net

One of the most important abilities of the human language faculty is recognition. This recognition ability enables us to classify what is or is not our native language, if the speaker is or is not a member of our own linguistic community, what is or is not a typical utterance or text, and eventually what is or is not safe. Our recognition ability is tuned by exposure to linguistic data, so that we normalize to what is familiar and react with caution to what is unfamiliar. Rare data is especially problematic because our safety detectors are not developed through prior recognition. With undeveloped or immature recognition strategies for problematic data, organizations and participants are equally vulnerable.

Since ancient times, as recorded in Joshua and the Book of Judges, well-attuned linguistic recognition strategies have been essential tools for safety, whereas poor recognizers have proven disastrous. Using language to prove group identity is a universal of politeness [1], but it is also a pretext which predators exploit. Internet predators are extremely, and deceptively, polite, formulating in-group linguistic strategies to ingratiate themselves with targets.

### Problematic Texts

The human language faculty's recognition ability is tuned to classify texts with which it becomes familiar through exposure. Some text-typing linguistic features are stereotypical and easy to spot (the formulaic "once upon a time" for a fairy tale), while other text-typing linguistic features are more subtle, (the ratio of nouns to pronouns for academic texts). Forensically-significanttext types are problematic simply because they are fairly rare. Through lack of exposure, most adults cannot reliably classify problematic texts, even if we have a generalized sense of danger, and certainly minors are even less equipped.

The ability to recognize and accurately classify different types of problematic texts has obvious survivability value. Imagine the disastrous effects of not being able to distinguish between:

- a real threatening chat and a phony threat chat, or
- a real suicide note and a phony suicide note, or
- an invitation from a predator in disguise with deceptive intent and one from a real friend

Other kinds of internet threats to minors that can be identified via linguistic recognition processes include but are not limited to:

- Cyberbullying
- Self –destructive or risky adolescent behavior
- Predatory solicitations and grooming tactics
- Authorship hijacking or impersonation within social networks, infomediaries
- Gang or cult recruiting schemes

ALIAS PRETEXT is the exclusive linguistic threat assessment technology offering that empowers minors, parents and organizations in recognizing potential health and well-being dangers on the Internet without compromising freedom of anonymity.

Accurate recognition can provide vital warnings to help insulate minors from potential harm and lead to evidence in criminal, civil and security investigations on behalf of parents and organizations that support virtual spaces where minors gather.

**The Keyboard Dilemma**

In an electronic society, the problem of problematic textsisaggravated by the fact that anonymity is attached to each keyboard. Even if competent digital forensics determines the address of the source computer, such information does not identify who was at the keyboard producing or targeting the victim of problematic communications [2, 3]. The keyboard dilemma thus adds to problematic texts the problem of authorship identification.

Internet safety for minors must include a technology for supplementing minor's immature linguistic recognition strategiesfor peer language patterns, classifying problematic text types, and determining anonymous or disguised authorship. Further, this technology must be validated empirically to meet legal standards for scientific and technical evidence. Finally, this technology should be accessible to both industry providers as a background support system and to parents, organizational safety and security investigation personnel as a forensic toolto identify perpetrators and threatening situations.

**PROPOSED SOLUTION: ALIAS PRETEXT**

We propose an automated linguistic identification and assessment system, ALIAS which provides specifically tuned linguistic recognizers for classifying suspect texts and authorship identification. These linguistic recognizers are built on statistical models developed from linguistic features. For each text, ALIAS quantifies sophisticated linguistic features based in syntactic, semantic and phonological theory. This quantification is then analyzed statistically using classification statistics (such as discriminate function analysis and logistic regression) or machine learning techniques (such as support vector machine and decision trees). The classification decisions are based on the statistical results.

**ALIAS solutions** provide a very rapid (milliseconds) assessment of a text. Currently texts can be file-scraped, web-scraped, or typed into ALIAS as a standalone application available through consulting services at ALIAS Technology LLC. By September 2008, the ALIAS SaaS (software as a Service) deliverable will be rolled out. The web interface provides parents, other guardians, businesses and prosecutors the ability to test suspect documents as threats.

Unicode-compliant, ALIAS is currently being used to analyze Urdu, Arabic, Russian, Korean and English texts.

In a chat or email monitoring solution guided by user consent, parental permissions or organizational terms of service, PRETEXT's architecture is designed to be interoperable across multiple platforms and a complimentary offering for many technologies deployed today.

**THE ALIAS PRETEXT Product Family** relevant to Internet safety includes:

- PRETEXT: assessing predatory features of texts
- ThreatAssess: assessing texts as threats
- Firepants: detecting potential detection
- SNARE: assessing texts as suicide notes
- UniAIDE: character-based authorship estimation
- SynAID: syntax-based authorship identification

As an example, ALIAS ThreatAssess determines if a text based communication is classified as a real threat or not [4]. Using a database of real threat letters from investigation or litigation and the Chaski Writing Sample Database [5]as comparison texts, a statistical model for classifying texts has been developed.Like the threat text type, each comparison text type has an interpersonal and emotional communicative purpose and therefore represents a good foil. Each new text fed into ThreatAssess is classified as either a real threat or a comparison type based on a leave-one-out cross-validated statistical model whose accuracy is reported in Table 1. Error rates can be calculated from the accuracies.

**Table 1: Cross-validated Accuracies for ThreatAssess**

| Accuracy | Differentiating Real Threat Letters from: |
|---|---|
| 97.7% | Simulated Threat Letters to Known Target |
| 91.5% | Simulated Threat Letters to Public Official or Celebrity |
| 98.9% | Letters of Apology |
| 100% | Love Letters |
| 97.8% | Complaint Letters |
| 97.4% | Angry Letters to Known Target |
| 96.1% | Angry Letters to Public Official or Celebrity |

**Cases**

In the shadow of Virginia Tech, a North Carolina investigation (2007) used ThreatAssess to confirm that a college student's email to his professor was not a real threat letter. In a civil investigation in Georgia (2007), ThreatAssess was used to classify an anonymous document addressed to a corporate executive. In Cahill v Schaffer (Delaware, 2006), SynAID was used to show that blog posts has been authored by at least two users of the computer identified as the source IP address. In North Carolina v Tew (2005) SynAID was used to demonstrate that Tew, a high school teacher, had indeed electronically authored love letters to a student on a school computer [3].

**Admissibility As Scientific Evidence**

Chaski's syntactic method for authorship identification SynAIDhas been admitted under the Daubert standard without any restrictions on her testimony as scientific evidence in Federal court (Green v. Dalton/US Navy,

District Court of the District of Columbia, Washington, DC, 2001) and under the Frye standard in several states. Chaski's method for threat assessment, using ALIAS_ThreatAssess, has been used in criminal and civil investigations since it was introduced in late 2007, but it has not yet been proffered as evidence in trial.

**EXPERTISE**

ALIAS Technology LLC and the PRETEXT product family grew out of Chaski's academic research and practical experience with applying linguistics to forensic investigation. The ALIAS system was built upon twelve years of research. Our unique service of using computational linguistics to build validated tools for handling language as evidence has allowed us to make a distinctive contribution to forensic linguistics, and to provide our clients with solid conclusions for investigative purposes or admissible evidence at trial.

**SWOT ANALYSIS**

**Weaknesses:**

- Limited recognition as SaaS provider and stakeholder in Internet safety solution

**Strengths:**

- Court recognized
- Peer recognized
- Empirically validated
- Proven solutions

**Opportunities:**

- Maintain and enhance strong core business
- Create consumer recognized identity for ALIAS
- Outreach to other child advocacy organizations

**Threats/Challenges:**

- Cases which require consulting beyond SaaS Copycat technology development

**COMPANY OVERVIEW**

The Institute for Linguistic Evidence Inc and ALIAS Technology LLC are sister organizations which grew out of Chaski's research in validating methods for forensic linguistics. Originally funded by the National Institute of Justice, US Department of Justice (1995-2004), the Institute for Linguistic Evidence (founded in 1998) provides an international forum for Chaski and research partners in the United States, Britain, Switzerland, Ireland, Canada, and Pakistan to develop and test computational methods for answering forensically-significant questions. Methods which have passed the scrutiny of validation testing are then incorporated into *ALIAS: Automated Linguistic Identification and Assessment System*.

Using this proprietary and patent-pending software, ALIAS Technology LLC(founded in 2007) provides consulting services to law enforcement, government agencies, corporations and private individuals. In addition to key members of the organization, ALIAS Technology LLC employs one full-time administrator and maintains contracts with several doctorate-degreed linguists and statisticians for data collection, management and analysis.

**Key organization members**

***Carole E. Chaski*** earned her doctorate in Linguistics at Brown University (1987), specializing in syntax, computational linguistics and language change, and has focused her research in forensic linguistics since 1992. She has programmed in mainframe, PC and Macintosh platforms.

Chaski has qualified as an expert witness, without any restrictions on her testimony, under the Daubert standard in the federal Courts of Georgia and the District of Columbia and under the Frye standard in the State Courts of Maryland, New Jersey, and California. Her reports and depositions have led to crucial evidentiary admissions in both criminal and civil trials as well as security investigations.

***Raye Croghan***is a leader in developing age and identity verification solutions, with more than 20 years' experience in business development from healthcare, financial services, IT and eCommerce. As founding partner of IDology, Raye is responsible for the vision of the company and verification product development. With dedicated focus on making the world and the Internet a safe place for children she is a well-known subject matter expert in the age and identity verification industry having held senior positions for products of Bank of America, US Bank, First Data, Verid and Gartner.

ALIAS technology development is led by ***Mike Faulkner.***With over 31 years of development experience (including nearly 20 years for AT&T's Bell Laboratories), Faulkner has previously delivered solutions for Lucent, Cummins Engine, Disney Imagineering, Eli Lilly, Universal Studios and General Motors.

**BUSINESS MODEL OVERVIEW**

ALIAS'PRETEXT business model supports businesses, government agencies, law enforcement, and consumers. In 2009, we have allocated 3 pro-bono programs for not-for-profit child advocacy type organizations, subject to approval, that would include up to a thousand PRETEXT reports at no charge. Outside the NPO pro-bono offering the cost for NPO's is $1,000 for an annual license of 1000 PRETEXT reports.

Commercial enterprises are charged for an annual license on a sliding scale basis based on their volume of revenue:

| Revenue | License Fee | PRETEXT Reports |
|---|---|---|
| 0-$1M: | $5,000 | 1,000 |
| $1M-$10M | $10,000 | 10,000 |

| | | |
|---|---|---|
| $10-100M | $50,000 | 100,000 |
| $100M+ | $100,000 | Unlimited |

The direct-to-consumer model for ALIAS PRETEXT is currently priced at an average cost of $100 per customer request and includes purpose verification and security checks of consumer users.

ALIAS PRETEXT is ideally poised to partner with complimentary web 2.0 solutions providers and InfoCard providers to enhance consumer consent-based technologies such as chat monitors, email filtering and child registry schemes. Collaboration with government, law enforcement, special interest groups and technology companies is invited.

**CONTACT INFORMATION**

RayeCroghan: rcroghan@gmail.com
T: 678-401-7630 C: 850-212-1824
4321 Old Cherokee St, Acworth, GA 30101 USA

Carole E. Chaski, PhD: cchaski@aliastechnology.com
302-856-9488
25100 Trinity Drive, Georgetown, DE 19947 USA

**CERTIFICATION**

I certify that I have read and agree to the terms of the Internet Safety Technical Task Force Intellectual Property Policyhttp://cyber.law.harvard.edu/research/isttf/ippolicy.

**REFERENCES**

1. Brown, P. and Levinson, S.C. Politeness: Some Universals in Language Usage. Cambridge University Press, New York, 1987.
2. Chaski, C.E. Who's At the Keyboard? Recent Results in Authorship Attribution. International Journal of Digital Evidence. 4:1. Spring 2005. Available at http://www.ijde.org
3. Chaski, C.E. The Keyboard Dilemma and Author Identification. In SujeetShinoi and Philip Craiger (eds). Advances in Digital Forensics III. Springer, New York, 2007.
4. Chaski, C. E. A Computational-Linguistic Approach to Threat Assessment. European Association of Threat Assessment Professionals Conference. 2008.
5. Chaski, C. E. Empirical Evaluations of Language-Based Author Identification Techniques. Forensic Linguistics: International Journal of Speech, Language and Law. 8:1. June 2001.