

# HOW TO INTEGRATE PRIVACY INTO CUSTOMER CARE



October 22, 2008

**Note: Please mute your phones to prevent interference. This webinar will be recorded.**



# AGENDA

- Compliance Overview
- Monitoring
- Watchdog Dispute Resolution
- Enforcement & Case Studies
- Q&A

# ENSURING PRIVACY AND TRUST IN A NETWORKED WORLD



# TRUSTE COMPLIANCE SERVICE

TRUSTe resolves over 5,000 Watchdog complaints a year.

Issues ranging from unwanted email and unauthorized profiles, to critical data leaks and even unauthorized credit card usage.

Complaints against companies small in size to large, well-known enterprise brands; from retailers to tax services and everyone in between.

100% complaint resolution rate.

100%!!!

# YOUR “BRANDING INSURANCE POLICY”

**Prevent unknown privacy pitfalls.**

- TRUSTe is here to detect weak points in your business practices or site that could result in a privacy threat, preventing escalation in the public eye.

**Extend your customer care with privacy.**

- Watchdog complaints are filed after a customer has first tried to contact a company directly – TRUSTe acts as a liaison between you and the customer facilitating recourse.

**Protect your brand.**

- TRUSTe provides the resources to help keep your brand a trusted one.

# MONITORING

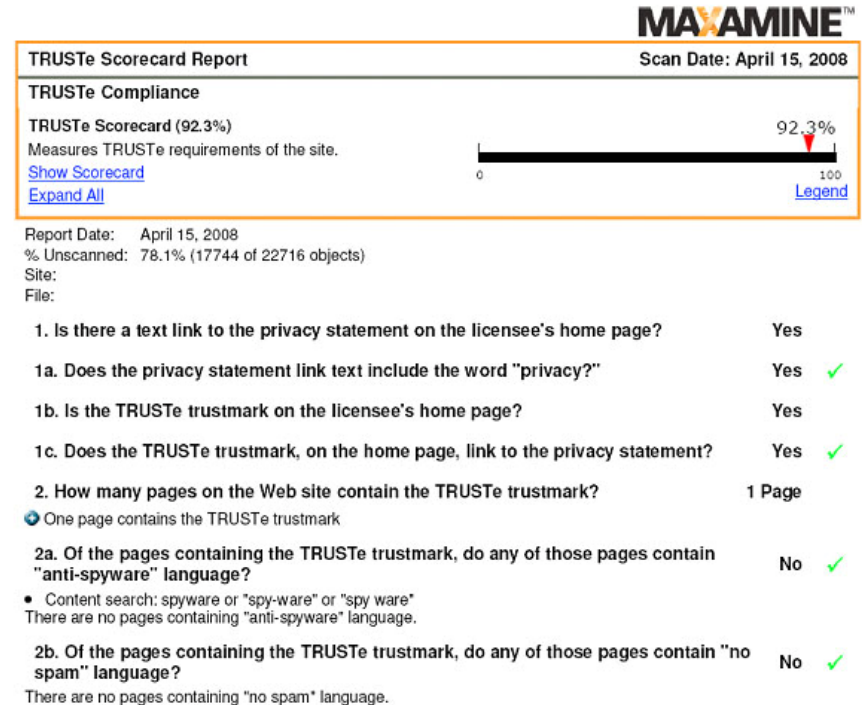
# WE KNOW WHAT OUR LICENSEES ARE DOING...

Avoid common mistakes – TRUSTe helps you review WHAT data you collect, and WHY.

- Collection and Use of Information
- Choice and your Web site's use of PII
- Choice and Sharing of Information with Others
- User Access to PII
- Security
- User Complaints
- Response to Legal Process
- Technical Information

# DIAGNOSTIC SCANNING UNCOVERS PRIVACY WEAK POINTS

- Undisclosed cookie usage
- Lack of security for sensitive information
- Lack of Privacy Statement link off homepage
- PII collection without a Privacy Statement link
- No privacy contact information provided
- Possible web beacon usage
- Bump-out if collects age



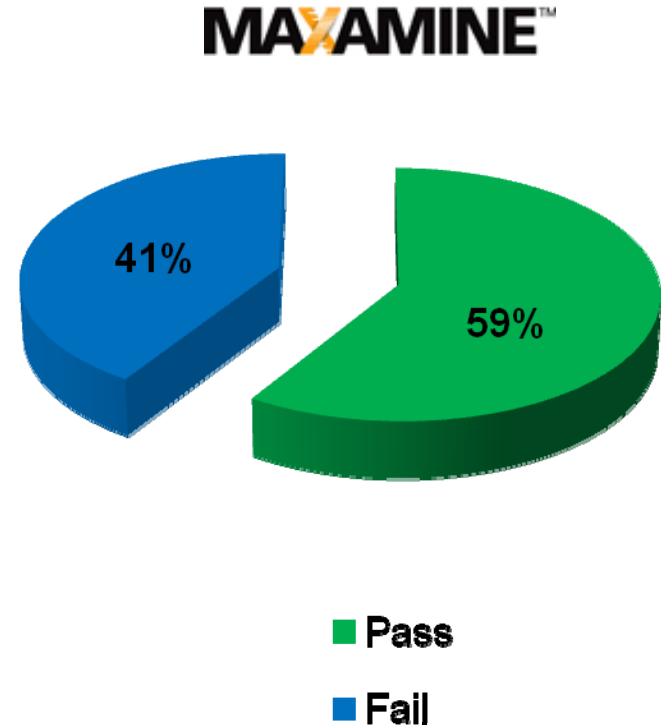
# PRIVACY RISKS THAT GO UNDETECTED....

- FTC CAN-SPAM unsubscribe violations
- Insufficient authentication procedures
- Lacking SSL encryption on password request pages
- Failure to delete online profiles due to process flaw
- Deceptive collection disclosures for importing user Address Book
- E-mail addresses leaked to third-party spammers via misbehaving partner
- Non-response to CA Shine the Light law inquiries
- Cross-site scripting vulnerability

# 2007 SCANNING PASS/FAIL RESULTS

Automated and manual monitoring of each Web Site's privacy statement and data collection processes.

- 59% overall pass rate on first scan
- Enterprise pass rate slightly lower at 52%
- Enterprise Web sites tend toward more complexity



# TRUSTE WATCHDOG



# WATCHDOG DISPUTE RESOLUTION PROGRAM

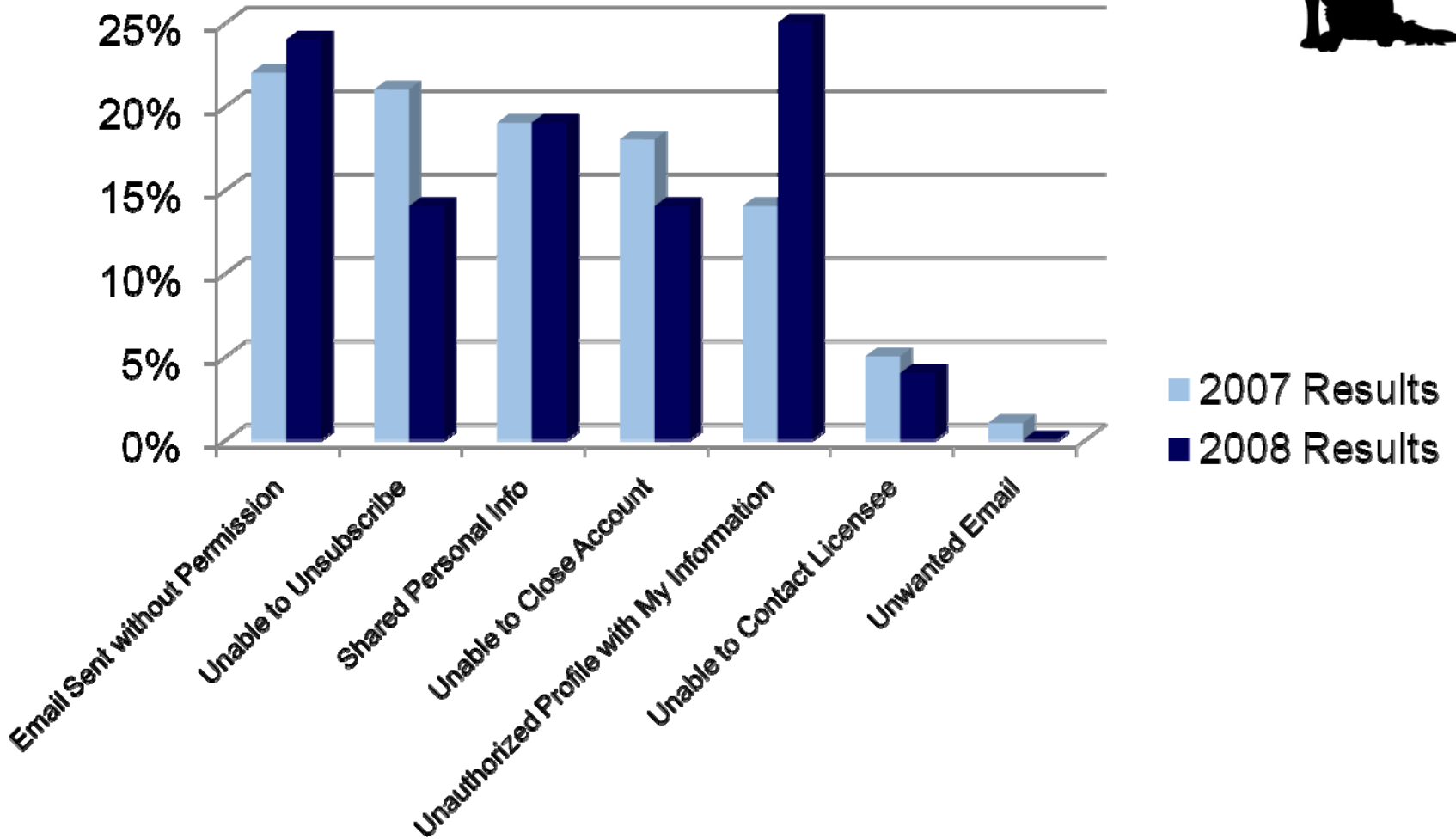
## CONSUMERS:

- Online independent recourse mechanism
- Specific to privacy complaints
- FREE of charge to consumers
- Easy-to-use online form
- Transparent, fair and equitable
- Complaints for offline data can be submitted by mail or fax

## SEALHOLDERS:

- Goal is to augment Sealholder's privacy program, escalate and resolve complaints quickly
- Watchdogs are confidential, there is no public posting of complaints
- Early security and privacy issue identification

# WATCHDOG TRENDS



# CONSUMER & SEALHOLDER FEEDBACK

“As always, TRUSTe sends a complete snapshot of what the complainant is stating; TRUSTe runs a very tight ship and we're lucky to be associated with you!”

- TRUSTe Sealholder



“I had no idea what to expect. I was delighted with the prompt acknowledgement of my complaint and the fast resolution of my problem.”

- Watchdog Complainant

“Within 48 hours of filing a complaint at Truste (about the classic closeouts ripoff), my credit account has been credited the full amount by classic closeouts (TWO unauthorized charges of \$69.99 each). If you have been a victim of this scam, file right away. You can find a link to truste at the classic closeout site. Looks like they have pull!!”

- Watchdog Complainant

# ENFORCEMENT & CASE STUDIES

# ENFORCEMENT PROCESS

Monitoring or Watchdog complaints triggers escalated investigation, which may include email seeding.

Sealholders are notified of non-compliance and given five days to respond with compliance plan.

In the event of non-compliance, or non-responsiveness, TRUSTe sends sealholder a certified letter of termination.

The Sealholder has 20 business days to fix the compliance issue to TRUSTe's satisfaction.

# ENFORCEMENT ACTIONS 2007

- Three terminations in 2007 where Licensee did not cure.
- Three decline to renew in 2007 due to “uncertifiable” business models.
- The vast majority of Licensees cure as soon as they are notified of an enforcement action or Watchdog complaint.
  - Committed to protecting their brand and consumer good will.
  - Don’t want to risk termination for cause and publication or referral.

# LEAKED “DO NOT EMAIL” LIST

In Spring 2008, the Watchdog System helped identify a security vulnerability of a leading tax filing Web site.

- Further information revealed the Tax firm had mistakenly made their DO NOT mail list public by posting to their FTP server.
- Upon additional investigation, TRUSTe verified the leak and notified the licensee.
- The licensee took immediate action and quickly remedied the situation.

The Watchdog Process helped pinpoint the source of the breach quickly, helping to minimize consumer harm.



# CHANGEABLE URL VULNERABILITY

In July 2008, the Watchdog helped discover a changeable URL that left consumer data exposed.

- The web site was unknowingly permitting a user to manually change the last few digits of his or her unique URL thereby granting the user access to sensitive identification papers of other individuals, including their passports.
- Company took immediate action – remedied vulnerability within **hours** and subsequently notified affected individuals.

The Watchdog helped licensee repair the problem, promptly preventing large scale data exposure.



# INCOMPLETE DOMAIN NAME

An incomplete domain name on web site allowed a rogue look-alike site to intercept sensitive consumer data.

- The licensee's web site error leaves an incomplete link pointing to the local name for the server.
- A rogue look-alike site is able to:
  - Intercept the web site's traffic
  - Duplicate the web site's look and feel to deceive consumers
- TRUSTe promptly verifies the Watchdog complaint and alerts the licensee.

Licensee arranges an emergency update to their web site that same evening to fix it and notifies users.



# TERMINATION: CLASSIC CLOSEOUTS

In June 2008 TRUSTe receives a consumer complaint indicating unauthorized charges to individual's credit card.

- TRUSTe analyzes licensee's consent process and security procedures.
- Licensee is suspended due to program violations:
  - Given time to cure violations and opportunity to be reinstated
- Licensee responds to some but not all cure items.
- On 9/23/2008 TRUSTe publicly announces Classic Closeouts' termination.

TRUSTe took immediate investigation actions and worked rapidly to obtain a refund for unauthorized charges.

# THE VALUE OF COMPLIANCE FOR TRUSTED DOWNLOAD PROGRAM

- Trusted Download Program (TDP) certifies downloadable software
- Most infractions in TDP are perpetrated by partners rather than Program Participants
- Controlling distributors / affiliates takes an active effort
  - A contract is not enough as there are incentives (\$\$) for abuse but low possibility of getting caught
  - Requires proactive, ongoing monitoring
    - Are the correct (or any) disclosures being served to consumers
    - Are consumers being presented with opportunity to provide consent
    - Is the download being promoted on approved locations
  - Technological control over the consent process
    - Referral URL's, consent mechanism
  - Solutions to verify validity of downloads
    - Audit download rate patterns, provide avenue for consumer complaints

# A TDP Enforcement Success Story

- comScore, RelevantKnowledge suspension July 2007
  - A rogue partner distributed the software before obtaining positive user consent
  - comScore removed rogue distributor
  - TRUSTe worked with comScore to develop a technological check on all downloads BEFORE install.
  - comScore fully implemented the solution across all distributors
  - Reinstated to program on April 2008

Details available on <http://blog.truste.org>

# PRESENTER BIOS

## John P. Tomaszewski

*General Counsel, TRUSTe*

John ensures that TRUSTe's compliance and enforcement efforts are thorough, transparent and defensible. Prior to joining TRUSTe, John served as Chief Privacy Officer of CheckFree Corporation and provided trust model consulting through his private practice.

**Email:** [johnt@truste.com](mailto:johnt@truste.com)

## Simona Nass

*Director of Compliance, TRUSTe*

Simona brings over 15 years of Internet-related privacy and technology experience. She previously served in high level positions at Red Hat, Internet service provider PANIX, as well as at other companies focusing on web services and e-mail.

**Email:** [snass@truste.com](mailto:snass@truste.com)

## Irina Doliiov

*Sr. Product Manager, Trusted Download Program*

Irina has over ten years of professional experience in Product Management and Marketing in the internet, software & professional services industries.

**Email:** [idoliiov@truste.com](mailto:idoliiov@truste.com)

**More info:** [www.truste.com](http://www.truste.com)

**File a consumer complaint:** <https://www.truste.org/pvr.php?page=complaint>