So you want to market your security product…

Terrell McSweeny
Aaron Alva

Federal Trade Commission

Black Hat 2017

Overview

Who is the FTC and why are we here?

Deception

Marketing 101

What should a security company do?

What should a security researcher do?

Recent developments re: product reviews and gag clauses

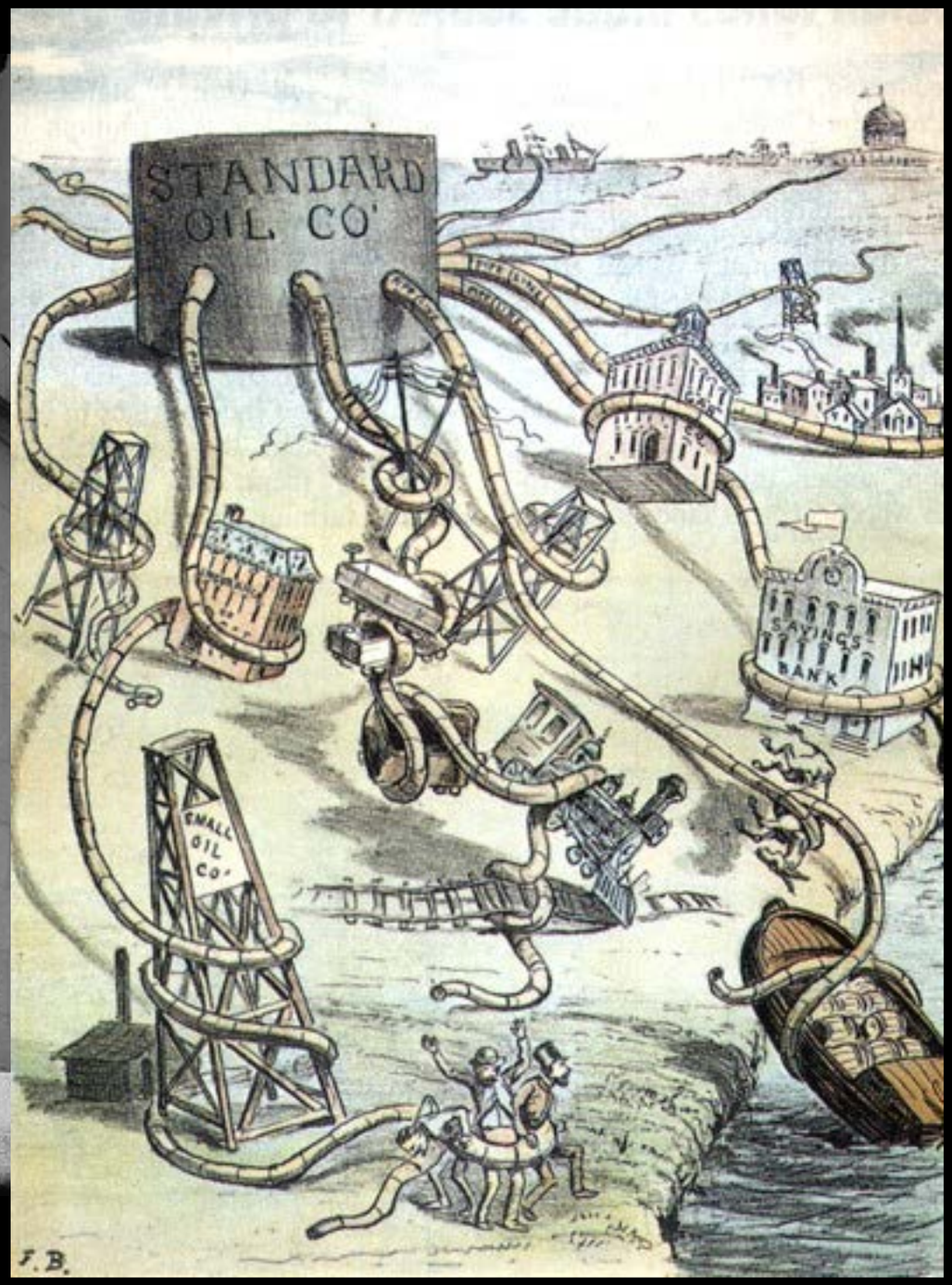
whois ftc.gov

- Commissioner Terrell McSweeny : Commissioner (@TMcSweenyFTC)

- Aaron Alva : Technologist, Office of Technology Research & Investigation (OTech)

These views are our own, and do not necessarily represent the views of the Commission.

whois ftc.gov



whois ftc.gov

Mission:

Consumer Protection

Ensure a fair & competitive marketplace for businesses

Tools:

Civil law enforcement actions

Policy activities (workshops, reports)

Consumer & business education

Research (OTech)

ID Theft
Smart TVs
Ransomware

Drones
Cross-device tracking

Marketing Security Products

FUD in the security market

Deceptive FUD

- E.g. Hayes Microcomputer Products, Inc. (1994)
  - Modem company claimed that modems without the “Improved Escape Sequence with Guard Time” would destroy data.
  - Not true, and ad showed that a time bomb may be lurking inside your computer.

TAKE AWAY: Even if you’re using hyperbole, you can’t misrepresent what your product does

Truth-in-advertising 101

Marketers of security products are subject to the same truth-in-advertising laws as all other advertisers

Truth-in-advertising 101

Tell the truth

The whole truth

Who is the FTC and why are we here?

Deception

Marketing 101

What should a security company do?

What should a security researcher do?

Recent developments re: product reviews and gag clauses

What is deception?

Three elements:

1. **Representation**, omission or practice that is likely to mislead the consumer.

2. Examined from the **perspective of a consumer acting reasonably in the circumstances** (and in the target audience).

3. **Material** (i.e. important to a consumer's decision to buy or use the product)

What’s a representation?

Types:

- **Express claims**
- **Implied claims**

Also:

- **Omissions**

What’s a representation?

Type 1: Express Claims

“G5 stores information in an SQL database, which… offers improved protection by storing your patient data in an encrypted format.”

But, software only used a weak obfuscation algorithm that could be unobfuscated without need for key or password.

(Henry Schein case, 2016)

What's a representation?

Type 2: Implied claims

Implied claim: KFC Original Recipe fried chicken breasts are healthier than a BK Whopper

BUT… potentially deceptive because, as a whole, KFC breasts have more trans fat, more cholesterol, more sodium, and more calories

MAN: Hey, honey. WOMAN: Hey. Remember how we talked about eating better?

Whole truth vs. half truth (Omission)

- Ad can be deceptive or misleading even it conveys info that is technically true— it can be deceptive by omission.

Whole truth vs. half truth (Omission)

- **E.g. Butterfly Labs**
  - Company manufactured and sold Bitcoin mining machines. Didn't mention that the company assembled machines, pooled them together, and used them to mine Bitcoin for *itself* before delivery to purchasers
  - This practice made it more difficult to consumers to mine Bitcoin for themselves when machines were finally delivered (if they were delivered at all)

TAKE AWAY: Don't leave out important info that would influence a decision to buy your product or service

Whole truth vs. half truth (Omission)

- E.g. Network Solutions offered 30 day money back guarantee

- But, deceptively omitted the cancellation fee

TAKE AWAY: Free means free. If people have to pay for it, it’s not free.

Who is the FTC and why are we here?

Deception

Marketing 101

What should a security company do?

What should a security researcher do?

Recent developments re: product reviews and gag clauses

Marketing 101

- Be honest about key attributes of your product or service
- Puffery vs. Deception
- Making claims? Have proof.
- Endorsements or certifications? Disclose who got paid $$.

Briefly: Unfair marketing

- **E.g. D-Squared**
  - D-Squared sent pop-up messages via Windows Messenger Service saying consumers' computers had flaw that enabled unsolicited popups

  - D-Squared sold anti pop-up software to disable Windows Messenger Service

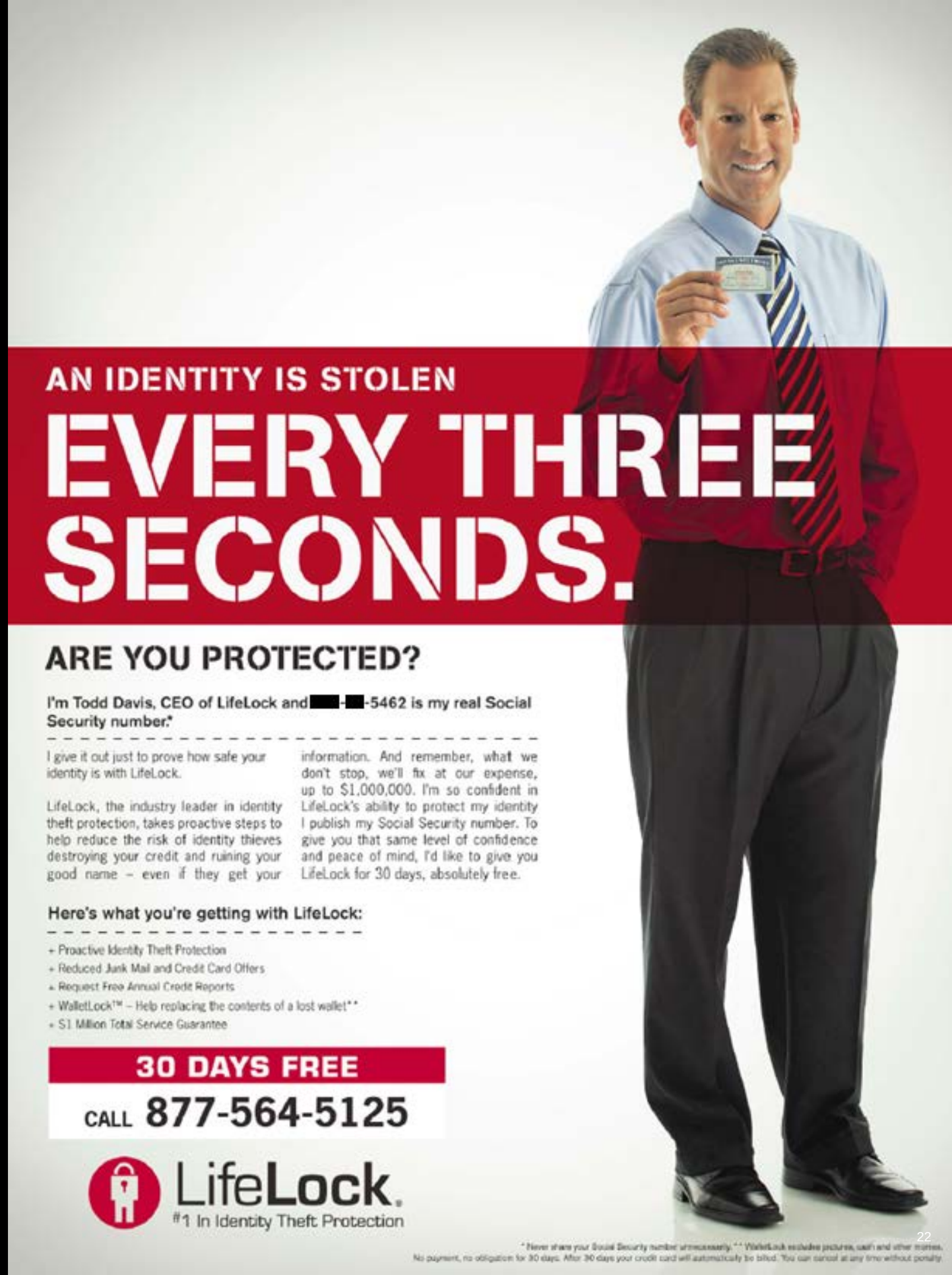
TAKE AWAY: Don't market your security product via a security flaw

Be honest about key attributes of your product or service

- Key attributes about your product or service (price, what it does, etc.) are material to consumers.
- If you make an express claim, it is *presumed* to be material
- Claims must be truthful and non-misleading.

- **E.g. LifeLock (2010)**
  - Falsely claimed it provided complete protection against all forms of identity theft by making customers' personal information useless to identity thieves.

TAKE AWAY: Don't make marketing claims that aren't true



Be honest about key attributes of your product or service

- E.g. In 1999, Apple's "Apple Assurance" product was offered to consumers for free so long as they owned the product.

- But, Apple started charging $35 to access support.

Be honest about key attributes of your product or service

- **E.g. Bonzi Software's Internet ALERT**
  - **"Download & Protect Yourself Against Internet Attackers Now - $49 (1 Year Subscription)"**
  - In fact, it only monitored 21 ports.
  - FTC complaint: "InternetALERT does not significantly reduce the risk of unauthorized access into computers and the data stored in them."

TAKE AWAY: Don't overstate what your product does.

Puffery vs. Deception

- “Electronic miracle”

  - Puffery; the FTC generally would not evaluate or pursue these types of claims

vs.

- “90% of security researchers think x security product is an electronic miracle that will protect your computer from zero-days.”

  - potentially actionable by the FTC

Making claims? Have proof.

- If you make any objective performance claims about your product or service, you need to be able to back them up with appropriate, reliable testing that is generally accepted in the industry.

Making claims? Have proof.

- **Example of claims that require substantiation:**
  - “Our product guards against 100% of known ransomware variants”
  - “The #1 selling protection among Fortune 500 companies”
  - “Protects against 20% more ransomware variants than competitor X”
  - And more

Endorsements or certifications?

Disclose who got paid $$.

- If a company has a material connection to a certifying body, or a person providing a review of endorsement – it has to be disclosed.

- A material connection would include:

  - A financial stake including

    - getting paid or compensated to provide a certification or endorsement,

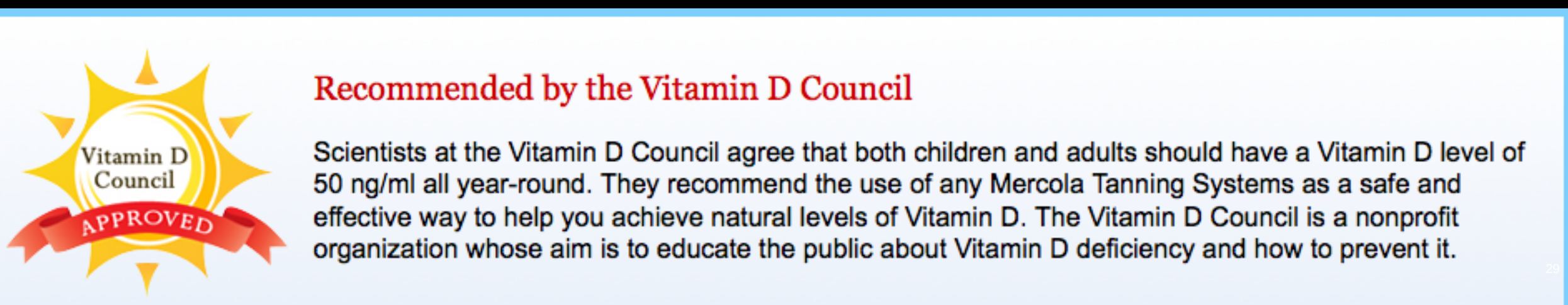
    - having an ownership stake in the company

  - A non-financial connection including certain types of relationships (e.g. endorser is a relative or spouse of an executive)

Endorsements or certifications? Disclose who got paid $$.

- Certifications: E.g. mercola.com (2016)
  - Manufacturer of indoor tanning beds claimed that the Vitamin D Council recommends the use of its tanning systems
  - Manufacturer paid Council for the endorsement

TAKE AWAY: If you pay the certifying body, disclose it. If you pay a certifier that doesn't actually have expertise, disclose that too.



Endorsements or certifications?
Disclose who got paid $$.

- Endorsements: E.g. Machinima (2016)
  - Video entertainment company (contracted by Microsoft to show products in positive light) hired influencers to show off new Xbox One and three video games.
  - Influencers were paid lots of $$ without disclosing payment.

TAKE AWAY: If they got paid – even reviewers and third-party websites – they need to disclose.

Who is the FTC and why are we here?

Deception

Marketing 101

So… What should a security company do?

What should a security researcher do?

Recent developments re: product reviews and gag clauses

What's a security company to do? (1)

- **List out your express and implied claims, and go through them.**
  - Make sure your marketing your ads or materials don't *imply* or leave the impression of something that isn't true from the perspective of a reasonable consumer.
  - Make sure your marketing department (if any) is on the same page as technical staff.
- Just because it's marketing doesn't mean you can lie or exaggerate!

What’s a security company to do? (2)

- Make sure your ads or materials you use to sell your product contain accurate info.
  - If you say you use encryption but only deploy basic obfuscation then that’s deceptive (Henry Schein case)
  - If you offer an SDK, make sure you aren’t deceiving developers by, for example, collecting BSSIDs for geolocation purposes when OS level location controls are not triggered (inMobi case)

What’s a security company to do? (3)

- Make sure you substantiate claims in your ads or materials.
- What substantiation do you need? Depends on the claim you’re making.

What’s a security company to do? (4)

- Make sure your endorsers disclose that they received $$ or value in exchange for their review.
- Make sure your certifications are not deceptive.

What’s a security company to do? (5)

- **Just because everyone else is spewing FUD, it’s not okay.**
- Let a self-regulatory body know (e.g. the National Advertising Division)
- Let us know.

What’s a security company to do? (Bonus: IoT edition)

- **Marketing an IoT device?**
  - If smart device stops while consumers expect similar 'dumb' device to still work, manufacturer should **disclose key use limits prior to purchase**
    - (Customers may reasonably expect an unsupported smart device to fail dumb)
  - “Manufacturers should consider whether they can disclose a *minimum* security support period.” Not just an “anticipated” time period.

Who is the FTC and why are we here?

Deception

Marketing 101

What should a security company do?

What should a security researcher do?

Recent developments re: product reviews and gag clauses

What’s a researcher to do? (1)

- Be on the look out for deceptive claims!

What’s a researcher to do? (2)

- Question claims:
  - Is there a potentially deceptive claim?
  - Is the company truthful about key attributes of the product or service?
  - Can the company substantiate that claim? (e.g. with numbers and a properly-conducted study?)
  - Is there a half-truth or omission?

What’s a researcher to do? (3)

- Let us know!
  - What was the claim? Show it.
  - What research did you complete that sheds light on that claim?
  - Is your research reproducible? How?
  - How is the claim deceptive based on the elements for deception?
  - How does this impact consumers?

What’s a researcher to do? (4)

- No, really. Let us know!
- File a complaint — see ftc.gov
- Send us your research — research@ftc.gov

New legal protections for security researchers

- Current DMCA security research exemption:
  - “So, if you meet all of the requirements, this temporary exemption allows you to test a connected toaster to assess the risk that an attacker might cause your bagel to combust or remotely monitor your toaster pastry habit.
  - But, of course, it does not authorize anyone to steal a toaster, hack into a neighbor’s toaster, or set toasters on fire in close proximity to flammable materials.”

DMCA security research exemption for consumer devices

By: Aaron Alva | Oct 28, 2016 2:12PM

Who is the FTC and why are we here?

Deception

Marketing 101

What should a security company do?

What should a security researcher do?

Recent developments re: product reviews and gag clauses

Consumer Fairness Review Act

The Consumer Review Fairness Act of 2016 (CRFA) protects an individual's ability to share her honest opinions about a business's products, services, or conduct, in any forum, including social media.

New law – Effective March 2017;
Enforcement starts December 2017

Consumer Fairness Review Act

The Act **voids gag clauses** that prohibit or punish consumers from publishing a:

- “a written, oral, or pictorial review, performance assessment of, or other similar analysis of” the contracted good or service.

Consumer Fairness Review Act

The law is new; FTC enforcement authority starts December 2017.

Gag clause cases prior to law's enactment:

- FTC:
  - Complaint against World Patent Marketing (alleging disparagement clauses are unfair)
  - Roca Labs (enjoining company from use of gag clauses that threatened legal actions against customers who wrote negative reviews about their weight-loss products)

- State Attorneys General:
  - NY AG case against McAfee seeking injunction preventing McAfee from "restricting the right to publish the results of testing and review."
  - NY AG case against Blue Coat for Blue Coat's anti-benchmarking clauses.

TL;DR

- Be truthful about the claims you make for your security product or service
- Question claims
- Stay in touch with us
- File a complaint — see ftc.gov
- Send us your research — research@ftc.gov