Protect Your Privacy and Online Identity

Sponsored by the Swampscott Democratic Town and the Swampscott Age-Friendly Committees

May 18, 2019

© Lutzker & Lutzker LLP 2019

LUTZKER
& LUTZKER
LLP

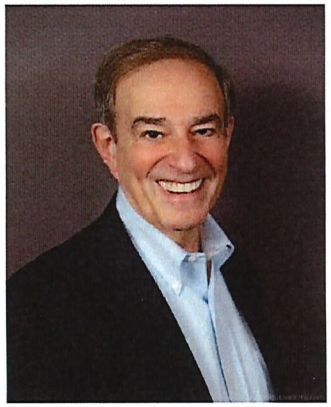
Legal Services for Businesses, Creative Professionals and Their Lawyers

Arnold Lutzker

Susan Lutzker

Attorneys and Co-Founders

Who are we?



LUTZKER
& LUTZKER
LLP

Arnold Lutzker

- Harvard Law
- 45+ years of legal experience in copyright and trademark strategy, protection, enforcement and policy

Susan Lutzker

- Georgetown Law
- 45+ years of legal experience in complex contractual matters and intellectual property protection and enforcement

What is the problem?

Technology, the First Amendment and our personal privacy are on a collision course

We are being bombarded with newspaper articles revealing the problems

How did we get here: a quick history

- 1950s – development of electronic computers
- 1962 – J.C.R. Licklider of MIT discusses his "Galactic Network" concept
- 1960s and 1970s– development of the Internet; role of DARPA
- 1980s – expansion of the Internet for educational use
- 1991 – development of the Worldwide web by Tim Berners-Lee and subsequent commercialization of the Internet

Where did things go wrong?

- The worldwide web was the perfect platform for distributing pornographic videos and photographs, creating a whole new industry
- Internet service providers (ISPs) like Netcom became concerned about their liability for content they did not create and sought relief through litigation and legislation
- The Digital Millennium Copyright Act (DMCA) passed in 1998 – ISPs are shielded from liability for money damages for copyright infringement if they comply with certain notice and takedown requirements
- ISPs have a free pass and become lax about screening requirements and privacy concerns
- Facebook, Google etc. have almost unchecked power

Boston Globe 3/8/19

WASHINGTON — Senator Elizabeth Warren proposed Friday to break up some of the nation's biggest technology companies, casting Google, Amazon, Facebook, and others as the newest villains in the scathing picture of capitalism run amok that has framed her political rise and her presidential run.

"They've bulldozed competition, used our private information for profit, and tilted the playing field against everyone else," Warren wrote in a 1,700-word online post detailing her plan... [emphasis added]

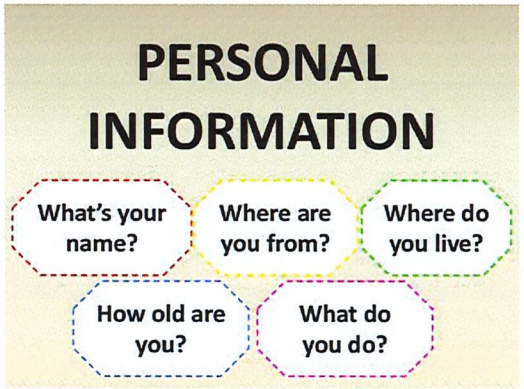
The good, the bad and the ???

- Ability to receive personalized news content
- Targeted shopping and location-based recommendations
- Emergency assistance
- Time savings
- Communities of support
- Powerful educational tool

- Identity theft
- Stalking
- Reputational damage
- Intrusive advertising
- Lack of transparency
- Arbitrary PII data retention (cannot be deleted)

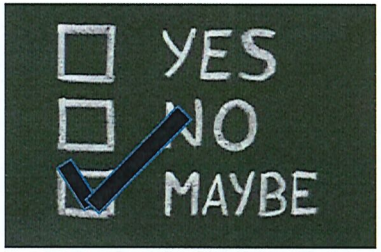
What constitutes personal information?

- Anything that identifies a specific person
- But – much broader than one would think
  - Information which, when combined with other information, can be used to identify a person
  - Anonymized information which can be re-identified
  - Information that relates to family members as well as an individual



Aren't there laws to protect us?

- In the U.S. there is no comprehensive federal privacy scheme
- No mention of privacy in the U.S. Constitution, but fundamental right developed over time ("The Right to Privacy," Samuel Warren and Louis Brandeis, 1890 *Harvard Law Review)*
- Some existing federal laws are sadly outmoded



Can't the federal government do anything?

- There are some efforts in Congress to enact legislation
- Senate Commerce Committee recently held hearings
- Some bills have been proposed:
  - Privacy Bill of Rights
  - Algorithm Accountability Act
- DON'T HOLD YOUR BREATH!

Contrast Europe

General Data Protection Regulation (GDPR)

- Went into effect in 2018
- Requires consent to collect personal data – must be freely given, clear and easily accessible
- Allows collection of only as much data as is necessary for the purpose
- Right to be forgotten and have data erased
- Narrow "legitimate interest" exception to consent
- Huge consequences for non-compliance – up to 4% of global income

States are taking matters into their own hands

- California Consumer Privacy Act of 2018 (CCPA)
  - Goes into effect in 2020
  - First generally applicable data protection law in U.S.
  - Will make covered businesses follow stricter privacy rules
  - No consent requirement as in GDPR
- Illinois Biometric Information Privacy Act
  - Guards against the unlawful collection and storing of biometric information – Rosenbach case
- Consumer data privacy bills are in play in at least 10 other states, including Massachusetts

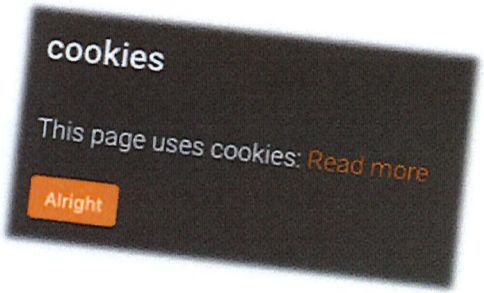
What's the story in Massachusetts?

- Massachusetts was the first state to enact heightened data security standards
- There is currently pending legislation to regulate the collection and sharing of personal information (SD 120, introduced by Senator Cynthia Creem)
- Some important cases have also relied on the more general MA Consumer Protection Act
- Massachusetts recently strengthened its data breach notification law
- There is also pending legislation to require companies to refrain from collection of personal and biometric data without express consent (SD 341)

What is surveillance capitalism?

It's the business model of collecting and selling personal data with or without consumer knowledge or consent and selling it to companies who want to profit from it!

A Common Data-Gathering Technique: *Cookies*



- Cookies are actually "breadcrumbs" left by websites
  - Requires notice and acceptance
- Pros & Cons:
  - Pro: Cookies are what allow your browser to "auto-fill" log in information when you go to a site you visit often
  - Con: Cookies lead to "web profiling"
    - Cookies can track what websites you visit, how long you stay on each site, when you leave or return to certain websites
    - Data gathered can be analyzed for recurring patterns in user behavior (good for targeted marketing)

Facebook

- Social media remains a central source of personal information data collection
- *March 2019* – Mark Zuckerberg posts an essay outlining "a privacy-focused vision for social networking"
- Facebook in the future will:
  - Facilitate private interactions
  - Feature "reduced permanence"
  - Allow encrypted messaging
  - Refuse to locate data centers in countries that have a poor record of protecting freedom of speech and human rights
- Facebook has already made the process of managing privacy choices easier

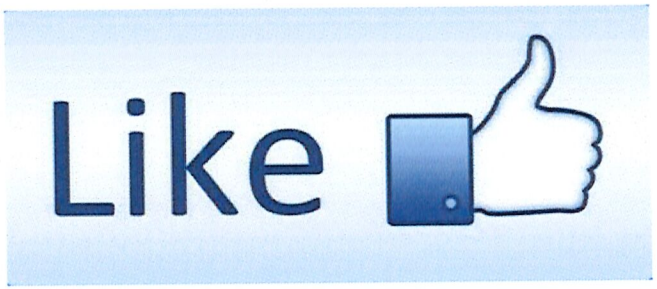
What led to Facebook's change of heart?

Lawsuits, fines, apologies, House of Commons hearings

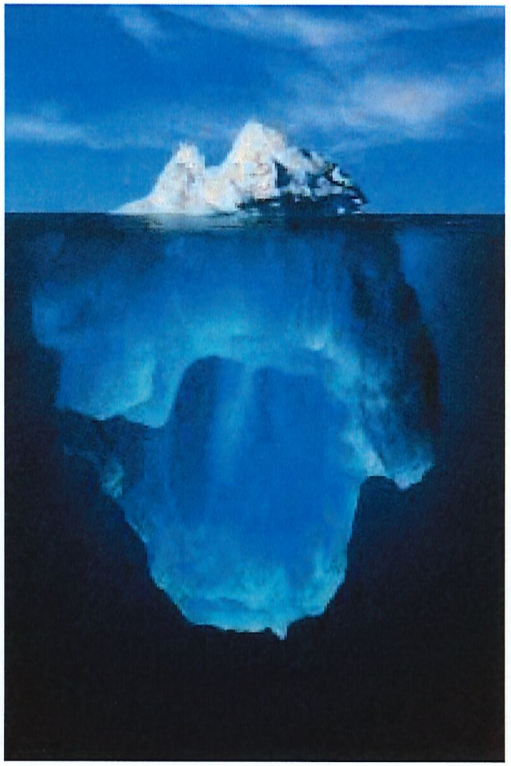
- Facebook facing multi-billion dollar fine from FTC for failing to abide by a 2011 consent decree to protect consumer privacy
- December 2018 – Facebook discloses that a bug may have affected up to 6.8 million users – allowed app developers to see photos users had uploaded but not posted
- September 2018 – security breach affected 15 million accounts
- June 2018 – glitch published the private posts of 14 million users
- May 2018 – Lawsuit against Zuckerberg by software firm claiming he "weaponized" the ability to access user data, leading to House of Commons inquiries
- March 2018 – whistleblower reveals that Cambridge Analytica improperly harvested the personal Facebook data of 50 million users to target for political ads in 2014

Will Facebook's changes make a difference?

- Encryption will reduce what Facebook can do to moderate content
- Auto-deletion of content may eliminate the Ralph Northam issue
- But…. Facebook will remain a massive and centralized source of power with little accountability
  - Anything you post, write, or like creates a digital footprint

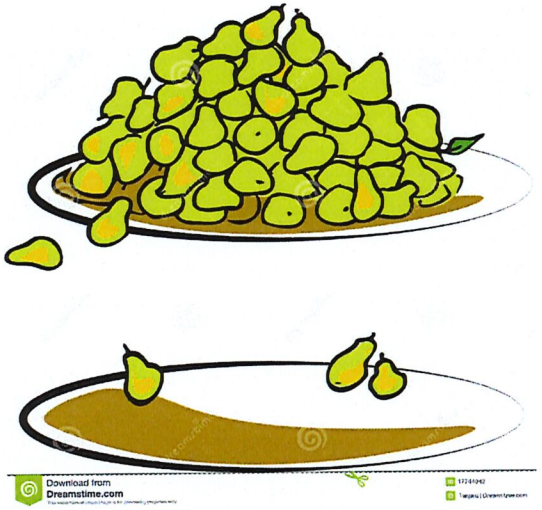


Facebook's issues are the most talked about, but they are the tip of the privacy iceberg



Our personal information is being collected every day and used in ways we never imagined or agreed to!

Here are a few examples....



DNA testing

- Providing information to a genetic testing company is providing information about family members as well as yourself
- There are provisions requiring consent, but privacy policies vary and can be changed
- But, with consent for research purposes, what if the research is about race and intelligence?
- Law enforcement (Golden State Killers case; FBI and FamilyTree)
- Data is anonymized before sharing but it can be re-identified
- GINA (Genetic Information Non-Discrimination Act) – notable omissions; for example, it does not apply to life, long-term care or disability insurance

Health apps

- A March article in the British Medical Journal reported that:

  "...evidence suggests that many health apps fail to provide privacy assurances around data sharing practices, and pose unprecedented risk to consumers' privacy, given their ability to collect sensitive and personal health information."

- In February the Wall Street Journal reported that "...many [popular health and fitness apps]were transmitting detailed information about topics including their users' weight and menstrual cycles" to Facebook.

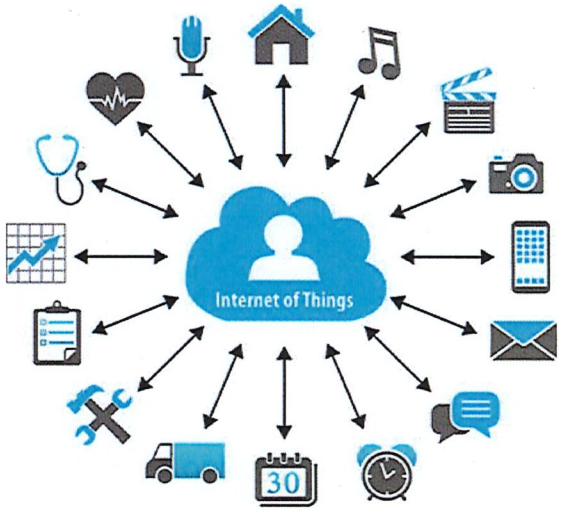
Drones for Commercial and Recreational Use

- Uses of commercial drones – construction or insurance inspection, filmmaking, mapping, real estate photography, product delivery
- Personal story
- Case law
  - William Meredith – Kentucky "drone-slayer"
  - Connecticut sunbather

- FAA position – none except to tell operators they need to be aware of state laws on privacy
- Singer vs. City of Newton – a federal district court invalidated parts of a city ordinance designed to protect privacy on the grounds that they conflicted with federal law on operational safety and licensing matters. But the decision leaves open the door to local regulation on the uses and nature of drones.
- Pending federal legislation

The "Internet of Things"

- **What is it?**
  - Network created by the computing devices regularly embedded in everyday objects
  - These objects can send and receive data
    - **Through sensors (how many steps did you walk yesterday?)**
    - **Through user input (what did you ask your voice assistant this morning?)**
- **Consumer products can become surveillance objects that track – and report on – people's everyday life.**



Virtual Assistants
(Amazon's Alexa – 100 million devices sold!)

- The devices record your words and send them to the cloud
- Amazon says that its assistants only store your "wake words" and that only you have access to the information
- Hard to be sure that the devices hear only what they are supposed to if they are always on
- Amazon employees listen to conversations to improve the product (AI)
- Embarrassing incidents in which Alexa made mistakes and sent recordings to places they were not supposed to go
- Chances for privacy invasion increase with compatibility with other devices (Amazon and Ring)
- Instances in which Alexa and Google Assistant talked to each other!
- Use of recordings as evidence in criminal cases - judicial warrants issued for Alexa recordings – pushback from Amazon

Isn't there a way to stop this?

- You can't stop Alexa from recording
  - 'Wake word' is *Alexa*
  - Assistant can 'mishear' and record when you don't want it to

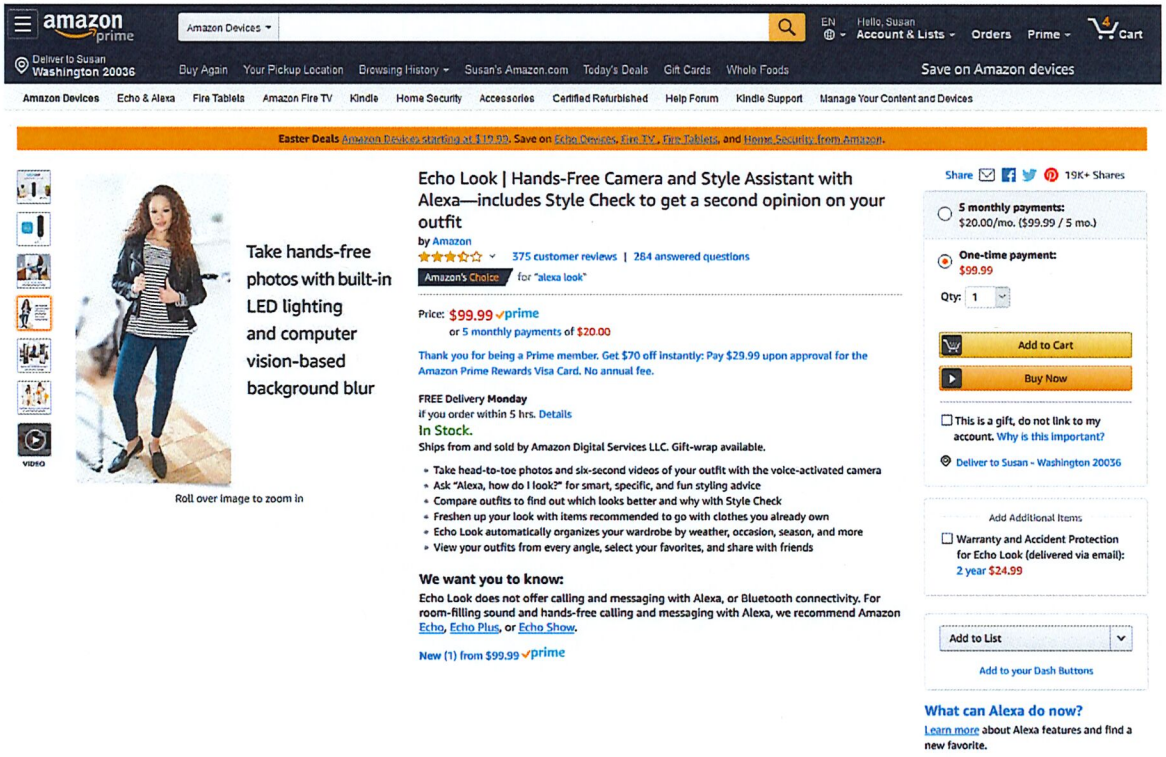
- You can manually delete past recordings, but
  - you need to know where to look and
  - you have to remember to keep going back

Amazon's Echo Dot for Kids

- Complaint just filed with the FTC alleging that Amazon is illegally collecting data on kids in violation of COPPA (Children's Online Privacy Protection Act)
- Essence of the complaint is that Amazon can collect a range of personal information from kids without the knowledge or consent of their parents because the parental controls are flawed
- May 9 – "Senators Markey, Blumenthal, Durbin, and Hawley Call for FTC Investigation into Amazon Echo Dot Kids Edition."

(Sen. Markey was one of the original authors of COPPA)

Privacy in the bedroom- assistant with a video camera collecting a range of information about you



But Google may have some answers

- Google changed its defaults to *not* record what it hears after “Hey, Google”
- But you would need to know how to change your defaults if your device predated this change
- Google also just announced that its "Hey Google" voice assistant no longer requires access to the cloud
- Google appears to have figured out a way to create a chip that contains sufficient processing power to provide users with wholly on-device speech recognition and assistance
- "Wholly on-device" removes the need for a personal device to transmit information to the cloud, which means that a user will no longer need Wifi access to use Google's voice assistant
- A user would have to have the new chip installed on their phone to access these capabilities

States to the rescue (again)?

- California Anti-Eavesdropping Act (pending in legislature) would prohibit devices from recording and storing conversations without consumer permission
- Similar legislation pending in Illinois

Cell phone tracking

- Contrast land lines
- What information is collected?
  - "near perfect surveillance"

- Status of the law – Carpenter v. U.S. – The Supreme Court declined to grant the FBI unrestricted access to a wireless carrier's database of physical location information without a warrant
- Following Carpenter, states are enacting laws imposing warrant requirements for electronic data
- Exceptions for emergencies, imminent physical risk

Geofencing

- In 2017 the Massachusetts Attorney General entered into a settlement with Copley Advertising LLC. The AG had alleged that Copley's use of geofencing violated the Massachusetts Consumer Protection Act.
- Copley had used geolocation technology to create a virtual fence around women's reproductive health care facilities, disclosing their locations to advertisers who then targeted them with ads based on inferences about their private information.
- Copley agreed to neither directly nor indirectly geofence the vicinity of any MA medical center.

Automated and connected vehicles

- GPS – by using you are consenting to a government-owned tracking system and willingly sharing your location information
- Autonomous vehicles capture a lot of information as to driver behavior (speed, braking pattern, collision information)
- 17 states have enacted legislation regarding data retrieval from EDRs (event data recorders)
- FTC promulgated best practices guide
- Seven Privacy Principles adopted by automotive industry
- Regulations proposed by National Highway Traffic Safety Administration to cover vehicle-to-vehicle communications

Doorbell Cams

- Amazon owns Ring and Google owns Nest
- Records image of everyone who comes to the door and sends it to the cloud without their permission (e.g., delivery people)
- "Smart" cameras use facial recognition
  - Becoming weapon of domestic abuse
  - Neighborhood social network that lets Ring owners share images of "suspicious" persons – implications for law enforcement
- Doorbell camera manufacturers able to collect information about you – target new products

Smart TVs

Vizio sued in California class action

Plaintiffs alleged that Vizio, without their knowledge, used automatic content recognition software to collect and report their content viewing histories to third parties !

Policing by facial recognition technology
Aggravating racial disparity?

The old way

- Surveillance footage from a store
- Smart phone video
- "Crapshoot method" of comparing to photos in database

The new way

- Amazon Rekognition
  - Scans face from security camera or video and compares the grainy image with database of photos from social media, jail mug shots, surveillance photos
  - Has resulted in many arrests
  - Technology still very imperfect
  - Built-in bias??? (for example, someone in a mug shot who was innocent nevertheless stays in the database, system more reliable for photos of people with light skin)

And the list goes on....

- Newborn screening – what if it is expanded to include adult-onset diseases?
- "Microdots" on printed documents that encode the serial number of the printer and the exact time of printing
- Google alliance with credit card companies to track the success of online ads
- Airplane cabins are about to get smart
  - Senator Merkley (D-Or) and John Kennedy (R-La) introduced the "Passenger Privacy Protection Act of 2019" this month
  - Bill to stop airline practice of installing microphones and cameras into seatback in-flight entertainment (IFE) screens

How about after we die?

- What is your digital legacy?
- In Europe there is a "right to be forgotten" – the Mario Costeja González case – Court of Justice of the European Union ruled that it was the responsibility of search engines to consider and honor requests from E.U. citizens to remove links containing personal information from search engines
- But in January 2019 an adviser to the Court recommended that Google be required to remove the data only from the results for searches made within the EU
- Slim prospects for similar legislation or court ruling in the U.S. – major collision with the First Amendment
- So it is up to individual data collectors: Facebook now offers an option to have your account deleted when you die or to designate a legacy contact to post message

What can we do?

On the personal level

- Read privacy policies so you know exactly what information is being collected, how it is being used and what your options are
- Be choosy about what social media you use and what information you knowingly disclose
- Educate yourself
- Follow recommendations to prevent identity theft

On the macro level

- Demand change: work towards a uniform public policy with uniform consent requirements
- Make candidates for political office address the issue
- Encourage industry efforts to reduce data collection, strengthen security and increase transparency