Employee Contact Tracing: Privacy, Public Safety, and Data Ethics

Jocelyn Aqua, Principal, PwC

Alexandra Ross, Director, Global Privacy and Data Security Counsel, Autodesk

Constantine Karbaliotis, Counsel, nNovation LLP

Session Description

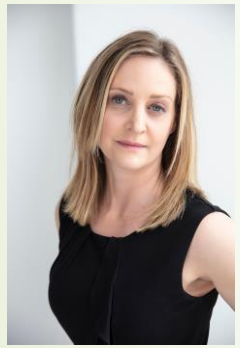
- In light of recent events, organizations (both public and private) are scrambling to help bring the COVID-19 outbreak under control, and are using all the mechanisms at their disposal. This includes existing tools such as CCTV and manual processes to check employees' temperatures, to use of data analytics and cellphone monitoring to track potential spread and contact points for illness and exposure. What are the privacy ethics in times of crisis? We will discuss how privacy professionals support this public emergency, while ensuring the proper balancing of employee privacy rights is maintained and that these measure are proportionate and effective.

Agenda

1. Introductions
2. Challenges faced by employers
3. Tools being used by employers
4. Technology tools and their challenges
5. Tactics: Human Factor and Technology
6. Public Policy Outcomes
7. Employer Consequences & Best Practices
8. Privacy and Ethical Challenges
9. Conclusions

Speakers

Jocelyn Aqua is a Principal with PwC based in Washington, DC, where she provides guidance to companies on the intersection of privacy, cybersecurity and regulatory risk. She is a former US government privacy official with over 20 years of public and private sector data privacy and cybersecurity experience, including 15 years with the Department of Justice, where she was responsible for assessing data systems and ensuring compliance with data privacy and cybersecurity requirements. Jocelyn also represented the Department in negotiations and consultations with the European Commission on cross-border data transfers, including the EU-US Privacy Shield Framework and the EU-US data protection privacy agreement for law enforcement exchanges of personal information. Previously, she was an attorney in private practice. Jocelyn currently advises global companies on implementing privacy and security requirements relevant to U.S. and EU data protection laws. She earned a JD from The George Washington University Law School, an MA from The George Washington University, a BA from Pennsylvania State University, and is a Certified Information Privacy Professional (CIPP).



Alexandra Ross is Director, Global Privacy and Data Security Counsel at Autodesk, Inc., a leader in 3D design, engineering and entertainment software. Previously she was Senior Counsel at Paragon Legal and Associate General Counsel for Wal-Mart Stores. She is a certified information privacy professional (CIPP/US, CIPP/E, CIPM, CIPT, FIP and PLS) and practices in San Francisco, California. She holds a law degree from Hastings College of Law and a B.S. in theater from Northwestern University. Alexandra is a recipient of the 2019 Bay Area Corporate Counsel Award – Privacy. Alexandra launched The Privacy Guru blog in January of 2014 and has published an ebook *Privacy for Humans* (available on Amazon and iTunes).

Constantine Karbaliotis is counsel at nNovation LLP, a boutique privacy law firm in Canada. Constantine has seventeen years' experience in privacy, on both domestic and international levels.. Constantine has fulfilled numerous roles in privacy, first and most recently as a consultant; Constantine has also acted as privacy officer and leader for two multinational organizations, where he managed the company's internal compliance and the development and implementation of privacy programs, dealing with diverse areas of international privacy and data protection. nNovation LLP is a virtual law firm with lawyers in Ottawa and Toronto delivering premium legal advice for a select group of clients, including leading businesses large and small, public sector bodies, industry associations, and law firms in other countries looking for Canadian expertise.

Challenges in the age of pandemics

- All business as well as public sector organizations, non-profits and charities are struggling to remain open during the COVID-19 crisis, and now re-open
- For many businesses, there is a stark choice – continue in some fashion, or face possible bankruptcy
- For others, layoffs and other significant reductions are already being experienced
- Public sector and non-profits/charities are struggling to meet their mandates and serve their constituencies
- All are trying to protect their staff from health & safety risks, to 'flatten the curve' and to ensure they mitigate potential claims against them

- General principles we must apply:
  - **Information collection must be necessary (effective) and proportionate to the harm we are trying to prevent**
  - **Just because you can do something, doesn't mean you should!**

Tools that employers are utilizing

Procedural/governance:

- Temperature monitoring
- Self-reporting
- "Whistleblowing"
- Contact Tracing (traditional)
- Information sharing with public health and other authorities
- Health 'passports'
  - Testing results
  - Presence of antibodies

Technology-based approaches:

- Contract tracing (device-based)
- Biometrics
  - Temperature
  - Other indicia
- Geolocation
- Facial recognition
- Too far?:
  - Always on web-cam

Technology Challenges

- Increased awareness/excitement about use of technology has created its own risks
  - Rush to use/create contact tracing applications
  - Apple/Google partnership
  - Inconsistency in app development and approaches
  - Lack of coordination
- Danger of implementing technologies that collect more data than is required
  - ClearView AI linking of contract tracing with facial recognition
- Trust issues where technology cannot be mandated by employers, or are dependent on public approaches, may undermine good uses of technology that help manage the crisis
- Even where mandated, technology can be circumvented by employees
- Technologies should ensure that COVID-19 is not spread (i.e. fingerprinting)

Tactics: The Human Factor

- Limit access to medical information to response team
  - Segregation of medical data from personnel files
- If communication to employees is required,
  - Give minimal information required to managed risk – avoid names
- Training and knowledge about security and privacy
  - More essential than ever in new ‘work at home’ world
- Consent?
  - Not always possible or defensible given relative positions of employees
  - Also must consider regulatory background (privacy but also employment legislation, human rights legislation) in information gathering

Tactics: Technology

- Security & safeguarding:
  - Data minimization – collect as little as possible
  - Security and logging to ensure proper controls and oversight, accountability
  - Equipping staff with appropriate tools to secure data (VPNs, encryption of hard disks)
  - Anonymization or pseudonymization
- Retention
  - Apply corporate retention policies
  - Otherwise dispose (securely) as soon as possible
- Minimizing sharing with third parties and government agencies
  - Document and ensure ‘legitimate purpose’

Public & Policy Outcomes

- Complaints and data access requests by employees (and others: consumers/customers, employee dependents)
- Risk of surveillance/ overreach/ authoritarianism
- Increased support for legislation for employee privacy
  - COVID-19 Consumer Data Protection Act – Senate bill proposed this past week
- Governance issues that will need to be addressed include how much data to share with public authorities, and when
- Private sector setting the tone? Google and Apple have put out terms of use for apps using their "Exposure Notification API":
  - only 'by or on behalf of gov public health authority'
  - 'Diagnosis Keys' *can* use identity to verify positive test cases
  - Location cannot be collected

Employer consequences

- Work @ home strategies resulting in potentially intrusive monitoring
- Collection of employee data that is unintended
- Insurance, performance impacts from ‘over-sharing’
- Insecure work @ home arrangements, lack of basic security understanding
- Lawsuits and regulatory actions for unintended on consequences, errors in judgement

Best Practices

- Consider regulator guidance carefully
  - In the uncertainty of the COVID-19 crisis, pay attention to what they are saying and recommend
  - Will be a defense to later armchair quarterbacking
- Leverage existing CMT and ethics programs
  - Your organization has resources that it can leverage - it's not *all* new
- Avoid grandfathering intrusive measures
  - Put time limits on technology and tracking
  - Ensure a review in a 'calmer' time
- Perspective:
  - Take a global rather than regional view
  - Treat people the same regardless of where they live

Privacy and Ethical Challenges

- Monitoring
  - Productivity measures
  - Monitoring of work @ home arrangements
  - Overly-intrusive monitoring (e.g. keylogging)
  - Impact on morale, trust
  - Highlights underlying issues in management of remote working
  - Is the technology actually effective?
- Retention and use of data outside original intended purposes
  - Discipline after crisis, effects on promotion
  - Health insurance coverage
- Unintended impacts from over-sharing:
  - Ostracization by fellow employees, discrimination
  - Creation of records by public health or law enforcement

Managing privacy and ethical risks

- Traditional risk-based approaches:
  - Privacy Impact Assessments
  - Cybersecurity Assessments
  - Business Continuity Planning/Disaster Recovery Planning
- Ethical data use:
  - "Ethics" or research types of oversight/governance
  - Engagement with stakeholders (employees)
  - Engagement with experts and advocates
- Common to both:
  - Transparency & notice, communications
  - Proportionality and effectiveness
  - Adherence to guidance from regulators, public health authorities
- Is a traditional PIA enough – without an ethics component?
- This situation highlights needs for ethical data governance that must last beyond the COVID crisis

Conclusions

- One of the biggest risks is that we fail to recognize some actions are needed in a crisis – but should not be the status quo
- We need to step back and determine what we have learned about ethics, governance, business continuity and organizational culture – and long-standing shortcomings -- to ensure we have better business resiliency without sacrificing privacy
  - A pandemic is just one kind of event – we have had others, and will again
- Employee privacy is no less important than consumer privacy – and being respectful of privacy is critical to maintaining morale and loyalty
- Events such as the COVID-19 pandemic will force greater awareness of the common interest of all employees, from executives on down, to the role organizations have in protecting employee privacy, not just because it is a legal obligation but an ethical imperative

Discussion

- Common questions & challenges
- Perspectives:
  - US Perspectives
  - Global Perspectives
  - Canadian Perspectives
- Q&A

Resources

- IAPP:
  - DPA Guidance on COVID-19:
  - Republican senators to introduce the COVID-19 Consumer Data Protection Act
- EU:
  - Decentralized Privacy-Preserving Proximity Tracing – Model DPIA
  - Hogan Lovells: COVID-19: Data Protection Interactive Map: Coronavirus in Europe
- US:
  - Ropes & Gray: COVID Tracing Alert
  - Brookings: Contact-tracing apps are not a solution to the COVID-19 crisis
  - Fastcompany: How COVID-19 is changing the way we think about privacy
- Canada:
  - Federal government unsure how PIPEDA fits with contact tracing app
  - Contact tracing efforts must respect citizens' privacy
- Australia:
  - Covid Not so Safe – the case for conscientious objection
  - I'm a privacy expert - and I've downloaded the COVIDSafe app