womblebonddickinson.com

WOMBLE BOND DICKINSON

Safe and Sound?

Protecting Employee Privacy and Company Data in the Era of Coronavirus

May 5, 2020

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Introductions

Tara Cho
Partner, Privacy and Cybersecurity
Womble Bond Dickinson (US) LLP
Tara Cho@wbd-us.com

Theresa Sprain
Partner, Employment
Womble Bond Dickinson (US) LLP
Theresa.Sprain@wbd-us.com

Robin King
Assistant General Counsel
Nuclear Fuel Services, Inc.
RMKing@nuclearfuelservices.com

Elizabeth Hope Cothran
Senior Counsel, HR & Employment
BWX Technologies, Inc.
EHCothran@bwxt.com

John Gambaccini (Moderator)
Partner, Corporate & Securities
Womble Bond Dickinson (US) LLP
John.Gambaccini@wbd-us.com

New Challenges and Competing Needs

- Urgency and uncertainty
- Getting the job done in a new way (at what cost?)
- Fast decisions and skewed judgment
- Unintended consequences / innocent mistakes
- Diminished or unpredictable resources and funding
- External stressors and new exposure points
- Ever-present bad actors seizing the opportunity
- Tensions between privacy and public health

Meeting Competing Needs

- Employee privacy can collide with the need or desire for transparency
  - Co-worker Safety
  - Public health
- Economic crisis and need to continue operations (not a free-for-all on the pre-existing legal requirements)
- Record keeping is necessary for compliance with old and new laws
- Legal guidance is still evolving—be reasonable and document
- Security can be a major challenge for employers with a remote work environment

Employee Privacy

Medical Information and Other Personal Data

- Employee information vs. patient data vs. plan participant data
- What is medical information / what information is subject to HIPAA / what is / is not protected information (ADA, HIPAA, etc.)?
- HIPAA misconceptions
- Other exposure points / sources of governance for personal data

Medical Information Disclosures

- Permitted and Required Disclosures
  - CDC-public health guidance on notifications
  - Public health overtaxed in making notifications
  - OSHA guidance on reporting
- Positive test results / suspected positive test results and employee privacy
- OCR waivers (first responders, business associates, etc.)

Non-Discrimination and Retaliation

- Think about it in terms of your existing treatment of individuals with medical conditions
- Given the grave concern over COVID-19, there is potential for greater discrimination and/or retaliation for individuals who had or were perceived to have had COVID-19
- Potential for unintended discriminatory results due to shifting operations

Employee Fraud and Misconduct

- Employee fraud and fraudulent records driven by:
  - Increase in telehealth services
  - Increase in available benefits
- Claiming positive test results to damage businesses or operations
- Snooping Employees

Employee Temperature Testing

- Formerly an impermissible medical test according to the EEOC
- EEOC changed its guidance in March in response to the pandemic
- Now it is a recommendation from the CDC for essential workers who have been exposed
- There is very little guidance on how employers should do this from CDC or otherwise

Recordkeeping

- Recordkeeping—is it necessary, and if so, how is it done?
- Think about whether a daily record is really necessary
  - If so, what is the purpose of keeping it?
  - If keeping it, what protections should be in place and for how long?
- Record keeping to mitigate future scrutiny or disputes or for insurance purposes

Employee Monitoring

- After an employee is out of work, how are you monitoring activity and productivity?
- Health and location monitoring
- Do you need to track employees still at work or who have returned to work?
- Google/Apple tracking apps and other contact tracing

Employee Privacy Notices

- What are you required to do?
- Do not forget state laws—California
- Consider the unintended consequence for not already being in compliance

New Data Sets, New Requirements

- Employee monitoring, temperature tracking and other new avenues of data collection create new types of data sets
- Obligations in securing and restricting use of data, retention and destruction
- Aggregate analysis of data

All Factors Have to Be Considered Together

- A corporate culture of transparency may not hold up to a pandemic
- The decision needs to be made early to avoid a perception of changing course
- Revealing too much—even a department—may identify individuals

The New Workplace

Business Continuity and Adaptability

- VPN and other remote network capabilities
- Availability of remote end user devices and equipment
- Load testing and backup
- Diminished resources and loss of funding
- Meeting contractual requirements and SLAs

Technology Services on the Fly

- Expedited vendor diligence (if any)
- Limited or reduced bargaining power
- Telecommuting restrictions and cybersecurity obligations in federal contracts

Security Outside the Perimeter

- Logical and physical security
- More remote devices, more exposure points
- More human threats / errors
- Lack of control over employee activities, downloads and application uses
- Blue-tooth enabled and other connected devices
- Subcontractors moving to remote workforce

Increased Cyber Attacks

- Email and SMS text phishing and malware attacks using COVID-19 messaging as bait via emails asking recipient to visit a website, open an attachment, click a link or similar

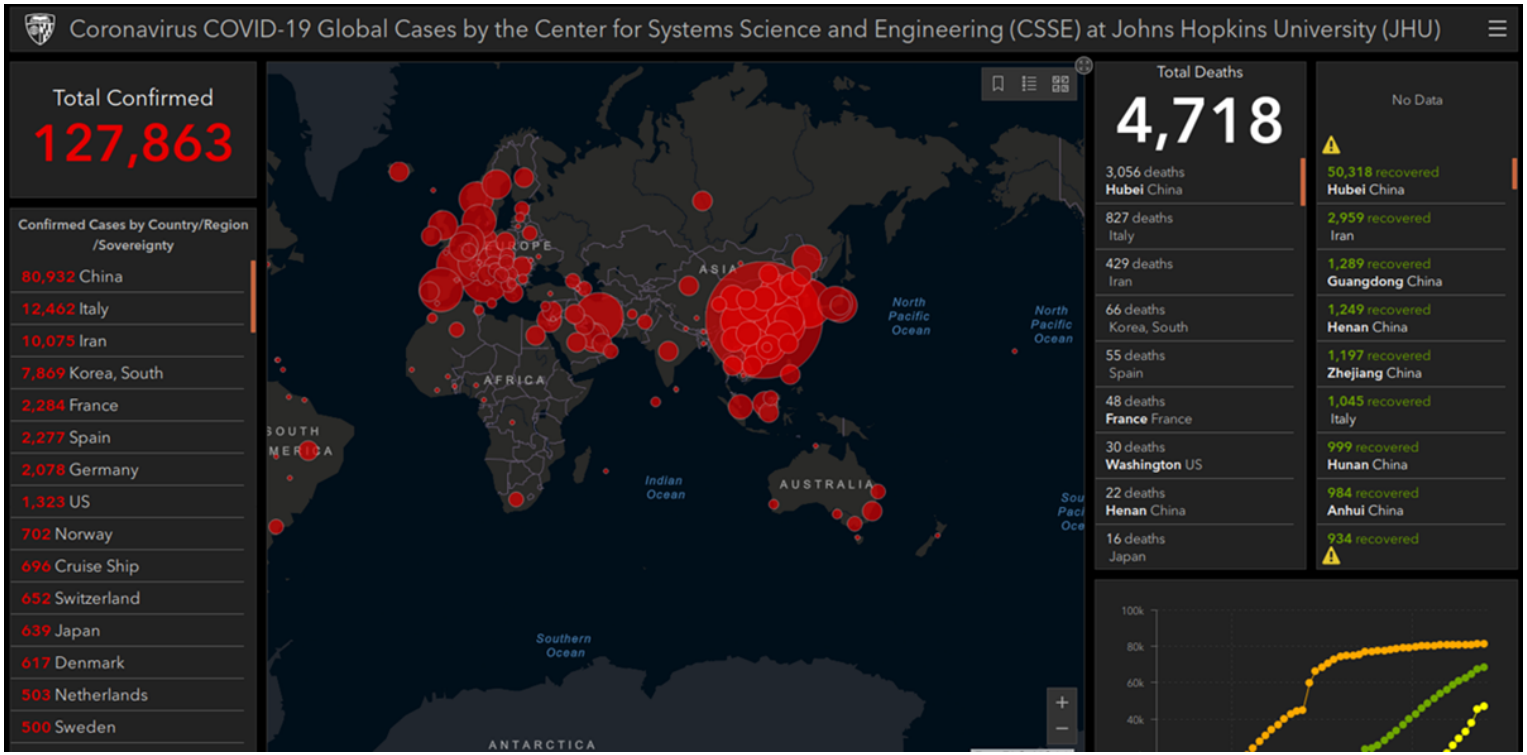
Source: Alert (AA20-099A) from U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the UK National Cyber Security Centre (NCSC) , April 8, 2020

Increased Cyber Attacks

- Attacks on telecommuting infrastructure and vulnerabilities
- Videoconference hijacking
- Fake charities
- Fake vendors / wire fraud
- Malicious software
- New domain names with COVID-19 related wording and fake sites that try to collect your personal information on sites that purport to provide:
  - The latest COVID-19 new and updates in your area
  - Outbreak tracking / positive cases in your location
  - Info or customized details on tax or other financial benefits

Increased Cyber Attacks

Malicious Website Example:



Source: Krebs on Security, March 12, 2020. https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/

Combatting Issues and Vulnerabilities

- Use secured connections
- Control screen sharing capabilities for meeting and require passwords
- Continue to vet software and restrict who can install/use new software
- Employee refresh training and reminders
- Tell employees where to look for accurate / reliable information
- Up-to-date software patching

See Appendix for other resources

Life After COVID-19: Return to Work

WOMBLE BOND DICKINSON

What Happens with the Data?

What should you do with the data amassed during the crisis?

- Some employee records will still be necessary for compliance purposes—tax credits for emergency leave, workers compensation claims, ongoing leave needs
- What can I delete?
- Consideration of record retention laws and policies

Employees Who Want to Continue to Work Remotely or Refuse to Return to Work

- NLRA/OSHA rights
- ADA accommodation to work from home?
- What physical measures/steps have been improved that might allow remote work where not allowed before?
- What have you learned about security that makes this not possible?

Returning Your Data to Work

- Transitioning the data from crisis mode/personal devices to normal operations and policies
- Start now to inventory who has this and what types of material
- Separating business from personal may be something employee does not want employer to do—how do we confirm?
- Certifications by employee

Transitioning to longer-term remote work

- If you're going long-term remote workforce, have you really fully vetted security aspects vs. band-aid?
- What policies are already in place?
  - Revisit BYOD and WFH policies
  - Some already revised in this time period to confirm use of BYOD/remind of confidentiality obligations
- What technology solutions do you need?
- Tracking devices and equipment
- Are there limits on remote access now that it is more ongoing?

Questions?

Speakers

Tara Cho
Partner, Privacy and Cybersecurity
Womble Bond Dickinson (US) LLP
Tara Cho@wbd-us.com

Theresa Sprain
Partner, Employment
Womble Bond Dickinson (US) LLP
Theresa.Sprain@wbd-us.com

Robin King
Assistant General Counsel
Nuclear Fuel Services, Inc.
RMKing@nuclearfuelservices.com

Elizabeth Hope Cothran
Senior Counsel, HR & Employment
BWX Technologies, Inc.
EHCothran@bwxt.com

John Gambaccini (Moderator)
Partner, Corporate & Securities
Womble Bond Dickinson (US) LLP
John.Gambaccini@wbd-us.com

Appendix

- FBI – Internet Crime Complaint Center Public Service Announcement about online scams: https://www.ic3.gov/media/2020/200420.aspx

- FBI Alert Re: COVID-19 phishing attack targeting healthcare providers: https://content.govdelivery.com/attachments/USDHSCIKR/2020/04/27/file_attachments/1436494/COVID_Phishing_FLASH_4.20_FINAL.pdf

- National Security Agency guidance on selection and secure use of telecommuting tools: https://media.defense.gov/2020/Apr/24/2002288652/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-LONG-FINAL.PDF

Appendix

- Health Sector Cybersecurity Coordination Center white paper on exploitation of videoconferencing services: https://content.govdelivery.com/attachments/USDHSCIKR/2020/04/27/file_attachments/1436539/TLPWHITE_UNCLASSIFIED_20200402-COVID-19%20VTC%20Exploitation%20%28002%29.pdf

- Health Sector Cybersecurity Coordination Center brief on COVID-19 related cyber threats: https://content.govdelivery.com/attachments/USDHSCIKR/2020/04/27/file_attachments/1436438/TLP_WHITE_UNCLASSIFIED_20200423-COVID-19_Cyber_Threats.pdf

- U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the UK National Cyber Security Centre (NCSC) alert on COVID-19 related cyber attacks: https://www.us-cert.gov/ncas/alerts/aa20-099a